DATA PRIVACY VS. MARKET POWER: NAVIGATING THE INTERSECTION OF PERSONAL INFORMATION PROTECTION AND COMPETITION LAW IN INDIA'S DIGITAL ECONOMY

- Mr. Manu Goswami[***]

ABSTRACT

*This paper examines the complex intersection between data privacy and competition law in India's digital economy, with particular focus on the Digital Personal Data Protection Act ("**DPDPA**"). As personal data becomes increasingly central to business operations and customer experience enhancement, understanding the impact of privacy regulations on market dynamics is crucial. The research investigates how DPDPA influences competitive activities and analyses how consent requirements may reinforce incumbent market positions. It also addresses the paradox of privacy-enhancing technologies (PETs), which while protecting user privacy, can potentially create barriers for new market entrants. The paper explores data portability provisions as a potential catalyst for competition while acknowledging their limitations. Through case studies of Indian tech firms, it demonstrates the practical implications of these legal requirements in operational contexts.*

The findings reveal that while data protection regulations are essential for consumer privacy, they can inadvertently strengthen the market position of established players who possess the resources to implement comprehensive privacy measures. The research concludes by offering recommendations on how India can structure its legal regime to achieve an optimal regulatory balance between data protection and market competition in its growing digital economy, emphasizing the need for policies that promote both privacy and competitive innovation while preventing the entrenchment of data monopolies.

Keywords: Data Privacy, Competition Law, Personal Data Protection Act, Digital Economy, India

[***] Mr. Manu Goswami is currently an LLM student at NALSAR University of Law, and can be reached at manugoswami@nalsar.ac.in.

I. INTRODUCTION

In the modern context, information has become one of the most valuable resources that pave the ways towards new economies and innovating customer experiences. Since organizations utilize personal data to improve services and clients' experiences, data protection and competition law have emerged as critical regulatory areas of concern. In India, this confluence has been best captured in the proposed DPDPA that seeks to protect personal data apart from addressing challenges of a dynamic digital economy. Nevertheless, the enactment of specific regulations regarding cooperations generates further questions regarding the nature of the impact on competition within digital markets.[1] The DPDPA outlines specific user control rights, the core of which is proportionate and informed consent for data collection and processing. However, while promoting privacy, this focus can also yield negative effects to competition. Larger organizations with a large array of consumer data held by primary tech firms can use this information to arrange for improved strategic standing, resulting in superior access to consumer data than small business rivals. Thus, as user consent is essential for the protection of personal data, it may contribute to the strengthening of the established players' market positions in the digital environment.

However, the current advancements in privacy enhancing technology add another layer of confusion. While they are presented as techniques for protecting users' information, some of these innovations may actually help the market leaders to strengthen their positions, thus locking out new entrants from the marketplace. When companies start to apply complex algorithms and artificial intelligence into their processes, thus using research and data analysis as a source of competitive advantage, there are fewer new products, services, technologies, and options for consumers. This paper discusses the various implications of India's DPDPA for competitive tensions in digital markets, including how consent frameworks shape market control, the complexities of delimiting relevant markets in data-centric industries, and the risks of privacy-protecting technologies' anti-competitive impacts.

[1] Rajvansh V, 'The Interplay between Data Privacy and Competition Law in India' (2022) 13 Journal of European Competition Law & Practice 291.

II. THE DIGITAL PERSONAL DATA PROTECTION ACT AND ITS INFLUENCE ON COMPETITIVE DYNAMICS IN INDIA'S DIGITAL MARKET

A. Overview of the DPDPA

India recently presented the DPDPA in 2023 to meet the challenges of data privacy, data protection, and digital rights of citizens with recommendations of the Justice B.N. Srikrishna Committee. Intended to protect individuals' information, DPDPA applies to data management and seeks to control how organizations gather, keep, process, and share individuals' personal information. It resonates with the increasing common trend of increased regulation of data to enhance user privacy following changes in the digital economies that see data as valuable assets with immense economic and competitive ramifications.[2]

i. Background of the DPDPA and Its Purpose of Protecting the User Information

The DPDPA is attributable to the need in handling data security and user anonymity as the Indian market experienced a breakthrough in the digital market. It lays down the basic concepts of consent, transparency, accountability, and collection limitation which forms the framework of India's legal landscape for personal data. The aim of the said Act is to prevent unauthorized processing of data and unauthorized use by providing a comprehensive structure for the proper handling of the personal data especially in the context of India market that is characterized by high dependency on technology, increasing number of mobile devices users, and growing literacy of the population in the digital age. Such factors have prompted the realisation that the safeguards have to be not just tough but also responsive to India's social and economic realities.

In its essence, the DPDPA provides data subjects, called data principals, certain rights with regards to their data, including the right of access, right of rectification and erasure of personal data, thus putting more regulatory responsibilities on the shoulders of data controllers.[3] The Act imposes consent-based rules, which tell that businesses have to obtain the clear consent of the data subject before processing their data with additional conditions for bio-metric data, health data and financial information. Therefore, as per the DPDPA's aim, it attempts to change the balance of

[2] The Digital Personal Data Protection Bill, 2023 <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.>.
[3] Naithani P, 'Analysis of India's Digital Personal Data Protection Act, 2023' (2024) ahead-of-print International Journal of Law and Management.

the power in favour of consumers while at the same time keeping corporations responsible for abusing data or undermining consumer privacy.

ii. Major Provisions Affecting Use of Data by Businesses and Internet Giants

1. **Data Fiduciary Obligations** - The DPDPA lays down the principle of data protection to be exercised by data fiduciaries which are the persons who are responsible for the processing of personal data. It categorizes data fiduciaries into two primary groups: types which include the significant data fiduciaries (SDFs) and general data fiduciaries.[4] High-risk SDFs which can be defined according to varying parameters such as data processing volume, dangers that data can pose to individuals, and revenue, are required to adhere to higher standard provisions that include data audit, impact assessment, and documentation of data processed, among others. This difference affects massive organisations that rely on big data and internet giants like Google, Amazon, and Facebook, which will be subjected to new regulations. From the compliance requirements highlighted above, it can be concluded that for many Indian tech companies, these compliance requirements could act as cost drivers which would reduce the competitiveness of the smaller firms, because the costs of compliance could prove to be resource intensive.

2. **Legal Obligation to Localize Data -** Among all the provisions, the provision concerning the mandatory local storage of some categories of personal data within the territory of India is one of the most discussed. Some of the personal data are allowed to be transferred to third country under certain circumstances while the key personal data must be stored only in India. This provision is motivated by reasons of national security but it is also pertinent to directly address issues of market competition. Some organisations, especially large MNCs which would otherwise incur the capital outlay for data centres could be better positioned to adapt while other firms, especially small players or start-ups may crumble under the added pressure.[5] The policy can also help to discourage international firms from accessing the local market and result in a concentration of market players that are able to meet the physical and organizational requirements of the data localization policy.

3. **Limitations and Regulation in the Gathering and Processing of Data –** DPDPA contains provisions for the principles of purpose limitation and data minimization to the end that data can only be gathered for a lawful purpose and only in the quantity that will be sufficient to ensure the said lawful purpose is realised. In addition, the Act required organizations to undertake

[4] Singh A and Anusha, 'The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach' (2024) 70 Indian Journal of Public Administration 502.
[5] Bareh CK, 'Reviewing the Privacy Implications of Indias Digital Digital Personal Data Protection Act (2023) from Library Contexts' (2024) 44 DESIDOC Journal of Library & Information Technology 50.

the privacy by design principles which demands that data protection should be incorporated in the organization's processes by design. It can restrain certain organizations from engaging in unbridled data collection and storage, which tends to be utilized for competitors' gain more often with targeted marketing or personalized services. While established firms especially those with well-developed ecosystems of data collection might still be using user data under DPDPA compliance smaller firms might not have similar abilities which could influence competition.[6]

4. **User Privileges & Permission -** The DPDPA focuses on the rights of the user to get consent to process data and to have control over the data. Requirements on the user consent state that the consent should not be influenced by other consents; it shall be informed and particular; the subject has the right to withdraw the consent at any time. This transfers the ownership of data from corporations to users and forces digital platforms to create the sound consent-management processes and data portability, rectification, and deletion. This may upset traditional business models based on the passive gathering of data and can pose specific challenges to companies in terms of engaging users. The cost and additional efforts for setting up such compliant consent management processes may pose as a threat to the business and depict small players at a disadvantage.

5. **Third-Party Data Use Implications -** According to DPDPA, the sharing of third-party data is prohibited specifically for other applications such as the constructing various user profiles, which remains pivotal for the digital advertising space. Businesses who use user profiling for targeted advertising or providing recommendations would have to decrease the scope and modify the procedures of third-party sharing and processing according to restrictions introduced. This could extend a headache to online businesses that solely depended on the advert revenues, calling for a change in the revenue generation strategies.

B. Shaping Market Competition and Innovation through Data Protection

The Digital Personal Data Protection Act (DPDPA) proposes significant shifts in data use practices in India, thereby placing the core concept of consumer privacy at the forefront of India's digital market. Beyond protecting user privacy, the DPDPA limits how firms gather, manage and warehouse personal information and, thus, impacts competitiveness and R&D among Indian technology companies. These data protection restrictions are expected to influence competition

[6] The Digital Personal Data Protection Bill, 2023 <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.>.

by forming opportunities and threats, which are expected to significantly influence Indian technological companies that are founded on data-driven methods.[7]

i. Examination of How Data Use Restrictions Affect Competition, Particularly Among Indian Tech Firms

The limitations on the use of data under the DPDPA for implementing higher standards and safeguards for data security, collection, and processing halt the unlimited data exploitation by many digital platforms currently. These restrictions will prove particularly disruptive for firms that base a significant amount of their business model on the harvesting and analysis of customer data for advertising, product suggestions, or market research purposes. For instance, the organization's principle such as the DPDPA that requires consent prior to collecting or processing any personal data undermines the way that these firms collect large amounts of user data that is crucial in building competitive algorithms. Small scale businesses in India may experience higher degrees of limitation as they try to increase the scope of their product portfolio with a percentage of the information that is available to giants such as Google or Facebook, respectively.

In addition, DPDPA lays down data localization, whereby certain types of data have to be processed and stored within the country.[8] For small firms, the cost and organizational requirements for constructing or obtaining local storage facilities are considerable. While established multinational firms will likely have the adequate infrastructure in place to absorb the costs, domestic firms particularly new and mid-sized firms may potentially find it hard to deal with the extra costs thus restraining their expansion. Data localization also elevates the position of large technology giants that are in a better position to meet the above standards and may attract users worried about their data security.

ii. Examination of Compliance Expense and its Effects on Entry and Exiting Further Obstacles and Existing Firms

Observance of the DPDPA will require investments, legal fees, technology acquisitions, staff sensitisation, as well as physical structural changes. Policies that require a firm to have an elaborate data protection strategy, data audit, and privacy by design and methods of obtaining consent, will be demanding for firms that have the resources to create these polices. However, political costs of

[7] How Will India's DPDP Act Impact E-Commerce Businesses?, *Ardent*, <https://www.ardentprivacy.ai/blog/how-will-indias-dpdp-act-impact-e-commerce-businesses/.>.

[8] Mishra A, 'Fundamental Rights and Data Protection (Balancing Innovation and Privacy in Light of Digital Personal Data Protection Act, 2023)' (2024) 13 International Journal of Science and Research (IJSR) 332.

compliance might hinder the development of potential entrants in the market by having high costs at the initial stages of competition, especially where firms are small startups who may not be in a position to afford such costs.[9] The costs and benefits of compliance do indeed appear to differ enough for this disparity to contribute to a continuing market consolidation process, given that incumbent firms tend to have considerably greater financial resources than firms entering the field from outside.

For instance, the creation of the categories of 'significant data fiduciaries' (SDFs) under the DPDPA places higher protective measures on firms dealing with substantial amounts of special personal data. Such requirement includes data audits, impact assessment at regular intervals, and documentation on the processed data. Although these measures increase openness and rigor, they equally give rise to the additional costs and requirements that are often unsustainable to new and small market players thus entrenching the incumbents through the mechanism of overly high barriers to entry through compliance costs.[10] Of this structure, there is creation of market that do not encourage the next generation players since entry barriers tend to rise for those who may want to grab a niche in the digital Indian economy.

The consent requirements under DPDPA add several regulatory layers to the market entry and innovation in digital services in addition to the ones created under the existing DP laws. Companies require stringent remedial process for obtaining prior and clear consent before collecting and/or processing of personal data. It also interferes with user interaction plans and data-based service development since firms now need to build processes that encourage openness more than efficiency. Although this is important to privacy this need hinders efficient data harvesting processes on which many small firms depend to provide efficient, real-time data-based services like marketing and behavioral analyses.

C. Privacy vs. Competition Law: Complementary or Contradictory Goals?

The legal relationship between privacy and competition law in India are a factor of concern since while they both seek to safeguard the consumers; they are rife with conflict when deployed in data-intensive markets. Basic legal instruments like the DPDPA are primarily used to protect individual rights in their information assets and regulate their use, thereby providing the users control over their assets. Competition law, on the other hand, aims at improving competition in the market,

[9] Sengar SS, 'From Pixels to Policies: Analysing the Provisions and Navigating the Complexities of the Digital Personal Data Protection Act, 2023' [2024] SSRN Electronic Journal.
[10] Singh A and Anusha, 'The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach' (2024) 70 Indian Journal of Public Administration 502.

eradicating such things as monopolies, and foul play by firms in the market. The desire for privacy, therefore, often results in restrictive laws that hamstring data as a competitive weapon, raising questions and concerns about whether the two goals can be so aligned.

i. Disclosure of Conflicts and Compatibilities of Data Protection and Market Competition

Privacy and competition laws have the same goal of protecting consumers at stake but have different set goals and operations. Combating the harms that privacy law seeks to remedy entails significant restrictions on data processing, with compliance costs that risk entrenching monopolistic power in the marketplace, thereby inhibiting competition. In this regard, though the large data controllers are in a position to bear the compliance costs, the exemption may hamper the dynamics and market innovation of the new players, entrants or smaller data controllers.[11] At the same time, privacy regulations give monopolistic advantages to dominating players who have the capabilities to proceed with stringent privacy regulations.

However, there is some overlap between the privacy and competition legislation as well. For example, requirements for data portability under DPDPA allow consumers to move their data to another service provider, which can thus lower switching costs and promote competition by allowing users to switch to more innovative or less concentrated platforms. It will be a very effective feature if utilized properly to provide level playing ground for the new entrants to compete with the large competitors by removing entry barriers related to data access.

ii. Measures for Companies to Strive for Privacy Compliance Amid Business Competition

The situation proves to be challenging for companies located in India as they strive to meet prescribed privacy standards while staying relevant in the market. Businesses need to function under conditions that strongly emphasize user permission and the right to know and protect their private data, even though this sometimes may slow down their processes and decrease their efficiency, especially in such industries where, for instance, time-sensitive data processing is necessary.[12] There shall be suggested legal and competitive adaptations, with companies potentially shifting towards privacy-by-design that integrates privacy into product design, thereby both meeting privacy laws and responding to competitors.

[11] Dixit P and Sharma S, 'Balancing Privacy and Competition: Evaluating the Competitive Effects of India's Data Protection Bill' (2023) 44 Statute Law Review.
[12] Gupta S, 'Interface of Data Protection and Competition Law in the Digital Economy' (2022) 3 Jus Corpus Law Journal 516.

Also, in response to such dynamics, companies may be forced to reconsider data-centric business models that prioritise data collection as a business driver, especially where data is no longer easily accessible as a result of data privacy laws. This may in turn translate to more reliance on other forms of growth strategies that do not conform to this monopolistic control of data, for instance; through the development of proprietary technologies, or by investing more in research and development. Companies can also consider joint data sharing contracts or can possibly develop software which complies with the DPDPA standards but is not significantly inferior in performance to the competition.

Lastly, based on the analysis one may conclude that both privacy and competition laws are capable to serve the consumer welfare interest; however their cooperation in the digital economy is seemingly far from perfect. Therefore, laws such as DPDPA can hinder market competition by changing the dynamics within which organisations engaged in data processing carry out their operations. These restrictions make the quest for the open competitive market, wherein new competition can enter the field and challenge incumbency, more challenging since some of the policies tend to solidify incumbency and raise entry barriers. On the other hand, if privacy and competition, especially in areas like data mobility, are aligned – there are new opportunities for the market participants to innovate safely and to build a more competitive digital ecosystem in India.

III. DATA PORTABILITY, CONSUMER CHOICE, AND MARKET COMPETITION

A. Data Portability as a Catalyst for Competition

India approved the Digital Personal Data Protection Act (DPDPA) that contains some provisions for data portability, one of the measures that would serve to promote consumer choice and competitiveness within the market of digital services. Due to data portability the consumers have the right to transfer their personal data from one provider to another in a structured, commonly used, and machine-readable format that can be exercised by individuals to switch between platforms easily without the loss of data. The portability requirements under the DPDPA are supposed to reduce the exorbitantly high switching costs in digital markets which at the moment, sustain the control of the dominant digital platforms.[13] The rationale for this approach is that consumers will be better equipped, and new entrants into the markets will be able to afford space to grow, leading to increased innovation in the digital markets.

[13] Sundara K and Narendran N, 'Protecting Digital Personal Data in India in 2023' (2023) 24 Computer Law Review International 9.

i. Understanding of Data Portability provisions under the DPDPA

DPDPA defines data portability under which data fiduciaries must provide individuals with means to obtain, receive, and transmit data to another data fiduciary of their choice. The type of data that can be ported from one service provider to another also includes entered by the user data, data collected during the provision of service or data taken from other activities occurred on the platform. More specifically, the protection of sensitive personal data and critical personal data—to which the DPDPA pays particular attention as special categories of personal information—should involve extra layers of protection and is likely to apply the exemption based on the freedom of portability owed to potential privacy concerns.[14]

Thus, the DPDPA's data portability provisions support similar provisions found in the EU's GDPR as it pertains to two of the most important parts of data rights and portability standards.[15] In turn, Indian users would benefit from enhanced forms of protection of their personal data, promoting a paradigm that focusing on the consumer and his/her autonomy in a digital environment. Data portability may lead to greater pluralism or variety of digital services that are aligned to consumer needs as firms compete to capture consumer attention in order to win their loyalty through provision of better or specialized services.

ii. Potential for Portability to Empower Consumers, Reduce Switching Costs, and Foster Competition

Such provisions must therefore be capable of directly influencing competitiveness indices by reducing the costs of switching between platforms, a determinant that underlines most platforms in the digital economy. In data driven industries, firms have traditionally used large user databases as a competitive asset, using data-driven methods to cultivate user loyalty and engagement through ROI-driven personalization, unique content and social networks. Most of such services work in what could be considered closed platforms, where users cannot easily switch to other platforms because of the data that they have accumulated.[16] For example, in social networking, online shopping, cloud-based collaboration applications and services, data portability would ensure that the consumer data identity including preference and usage history and customized settings could

[14] Pankhudi Khandelwal, 'The story of data portability in India: a lack of clarity under data protection, competition law and other frameworks', (2024), *Law School Policy Review* ,<https://lawschoolpolicyreview.com/2024/11/27/the-story-of-data-portability-in-india-a-lack-of-clarity-under-data-protection-competition-law-and-other-frameworks/.>.

[15] Malhotra C and Malhotra U, 'Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India' (2024) 70 Indian Journal of Public Administration 516.

[16] Naithani P, 'Analysis of India's Digital Personal Data Protection Act, 2023' (2024) 3 International Journal of Law and Management.

be easily transferred across service providers making it difficult for firms to control and raising the stakes for service quality and data privacy.

Approaches to decrease the switching costs are good for consumers and smaller firms or startups that have limited access to users' information comparing to the large-scale players. Having portability rules in the background, new start-ups may be more likely to secure consumers who used to avoid dependency on enormous, well-developed platforms. This dynamic encourages a system of competition which ensures that any firm no matter their size will be competing on the quality, the level of disclosure and the value of what they offer as opposed to holding exclusive access to relevant data. Smaller firms may also adopt unconventional, customer-centric product strategies that enable them to target and consolidate relevant customer segments by integrating data and information into their services more conveniently and from anywhere than in large firms' ; effectively using this advantage to appeal to customers who are looking for relevant, smaller applications or services as alternatives to ubiquitous platforms.

iii. Implications for Market Competition and Innovation

The facilitation of data portability is expected to stimulate market competition in two significant ways: it also puts pressure for innovation in the established players due to the increase of competition and allows the small players to distinguish their services with the customer-oriented solutions. When switching costs are lowered, the incumbents face loss of the erstwhile exclusive data advantage which leads them to improve their product offerings and the customer experience in the market continuously. Data portability can also be viewed as an initial point of entry for smaller companies to tap into consumer trends of privacy, transparency, and personalised services currently pushed in digital domains.[17]

Nonetheless, the portability provisions can engender cross-industry coordination and interoperability standard, and a system where the different companies participate in constructs to allow a user-directed control of data transfer. The incentive of the cross-platform compatibility returns the industry to a diverse and more open platform environment, thus compensating for monopolization strategies and offering more service variety for consumer benefit. For instance, data portability could be applied to banking as a service where consumers could take their data from one digital banking service provider and move it to another to spur innovation in a sector where few players control the market. Likewise, health tech companies can use portability to enable

[17] Dixit P and Sharma S, 'Balancing Privacy and Competition: Evaluating the Competitive Effects of India's Data Protection Bill' (2023) 44 Statute Law Review.

patient records to be easily transferred from one care provider to another to improve data flow while at the same time promoting the advancement of service delivery and availability.

B. Consumer Choice and the Limits of Data Portability

i. Effect of Data Portability on Consumer Decision Making

plans such as data portability intentions as provided by India DPDPA are considered good for the consumers by allowing the moving of the personal data. This capacity in theory reduces the barrier to entry for consumers when switching between service providers and should in principle promote consumer power competition. Because consumers are no longer locked into a given platform, as they may have been in the past with their data, portability empowers them to consider different choices, thus potentially driving competition as platforms seek to retain or gain users' data through service quality, security, and customization.[18]

In digital services markets, such as e-commerce, social networks, and financial services, consumers' decision-making process is highly dependent on how introduced services utilize personal data to provide tailored offers. By becoming portable, consumers do not feel that they will lose all the built-up personal data such as contacts, preferences as well as previous records, therefore freeing the users to move around and compare providers. Moreover, this capability can enhance the effect of forces that increase transparency by making consumers pay attention to privacy policies and services provided by various platforms, creating a more competitive environment.[19]

Nevertheless, the effect of portability on the freedom of choice for consumers is also conditioned by the consumers' awareness of such mobility and the degree of ease with which the data can be transferred. Some of the general limitations could include; Data format restriction in portability rights, this indicates that to enhance this right, regulatory authorities should ensure compatibility. If these scenarios are not implemented, consumers may stay with large platforms despite inexpensive portability due to perceived ease of switching.[20] Even if services are highly interdependent and intertwined or include exclusive content, there are tools that can prevent

[18] Naithani P, 'Analysis of India's Digital Personal Data Protection Act, 2023' (2024) 3 International Journal of Law and Management.
[19] Farhad MA, 'Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry' (2024) 48 Telecommunications Policy 102836.
[20] Dixit P and Sharma S, 'Balancing Privacy and Competition: Evaluating the Competitive Effects of India's Data Protection Bill' (2023) 44 Statute Law Review.

consumers from switching, so that the mere portability cannot overturn consolidated preferences in the market.

ii. Risks and Limitations of Data Portability: Likelihood of Data Integration

Although data portability can unlock competitive scenarios there is a tendency that it could contribute to entrenchment of dominant platforms. It is perfectly understandable that the facility to compile enormous volumes of sound that have been procured from varying sources can be both an advantage and disadvantage. On one hand, it may open an opportunity to level the playing ground to the extent of allowing small players into the market and develop new technologies. At the same time it can result in data aggregation in the hands of large technological companies who possess the technical capabilities to effectively manage big amount of user data and capable to generate revenue out of the data via superior analytical tools.[21] This accumulation of information can bring new levels of personalization and ease for the end user, yet solidify these platforms credit even further through access to perpetually expanding databases that individual firms may not match.

One such data concentration risk is most evident when larger platforms use portability to improve cross-service cohesion to gain insights into consumers' actions across different verticals. For instance, a single prominent e-commerce system that implements integration with social networks may use the information about interactions in these networks to manipulate purchasing behaviour further cementing its grip.[22] While this practice adheres to data portability rules, it has the side effect of deepening market consolidation as consumer data is concentrated in few platforms making it difficult for new entrants to compete with firms who possess similar insights.

There is also the danger that dominating platforms will use portability options to establish "data traps" where consumers move data from several sources to a single platform that gradually takes over all users' information.[23] Thus, data portability can ironically only strengthen data oligarchies, particularly in a market where the incumbent may not have adequate resources to accommodate the constant big data migrations, or may not provide sufficient privacy guarantees. This

[21] Kumar A and Sharma R, 'Comparative Analysis of Data Protection Laws and Ai Privacy Risks in Brics Nations: A Comprehensive Examination.' (2024) 13 Global Journal of Comparative Law 56.
[22] Engels B., 'Data portability among online platforms. Internet Policy Review' [Internet]. 2016 [31 December 2024]; 5(2). <https://policyreview.info/articles/analysis/data-portability-among-online-platforms.>.
[23] ibid.

phenomenon calls for high data protection norms in the case of portability to ensure that dominant participants do not capture data at the cost of consumer option and market competition.

C. Comparative Insights from the GDPR on Data Portability

i. Overview of the EU's Experience with Data Portability and Its Competition Effects

The EU's General Data Protection Regulation (GDPR) introduced data portability as a right in 2018, making it one of the first jurisdictions to formalize this concept into law. Article 20 of the GDPR mandates that data controllers provide individuals with the right to transfer their personal data to another controller in a structured, commonly used, and machine-readable format. The application of data protection in the EU has provided some evidence on its competitiveness and, consumer consequences, especially for digital markets. So, GDPR's data portability has empowered consumers by giving users greater control of their data trail and the ability to share this data with rival services. However, the progress it has made has been a little lacking majorly attributed to the issues of centrally controlling the process due to standardization as well as high cost had forced SMEs to compromise on the necessary measurement compliance costs.[24]

In the EU, where data portability has gained currency for large firms to ensure competitive practices in consumer remains engaged. For instance, the social media industry and telecommunication business have experienced slow over changes in the offer of privacy-centred upon features within products due to firms wanting to satisfy consumers with stronger preferences towards privacy. Yet, research shows that data portability does not exert significant competitive pressure, or to put it differently. While consumers have benefited from this rectitude, the absence of broad technical specifications and suitable rules of interface has made transfers across services uncoordinated, which in effect has reduced the operational usefulness of portability rights.

Furthermore, portability rights available under GDPR have become very compliance consuming for SMEs, which may find it difficult to interconnect with the large platforms for data transfer. The disparity in compliance capability has inadvertently favoured larger companies that possess the infrastructure and technical know-how to facilitate data portability.[25] As a result, the GDPR's data portability provision has not been as transformative for market competition as initially

[24] Reimsbach-Kounatze, C., A. Molnar (2024), 'The impact of data portability on user empowerment, innovation, and competition' *Going Digital Toolkit Note*, No. 25 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf.>.

[25] Gill, D. and Kerber, W., 2020. 'Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data'. *Opportunities, and the Need for Going Beyond the Portability of Personal Data (October 11, 2020)*.

anticipated, largely because dominant firms still control vast amounts of user data and can dictate portability practices.

ii. Key Learnings Applicable to India's Market and Regulatory Landscape

India can draw several insights from the EU's experience with data portability under the GDPR to inform its own regulatory landscape. First, India's DPDPA should prioritize establishing standardized data formats and interoperability frameworks to facilitate genuine, user-friendly portability. Without such standards, as seen in the EU, the operational benefits of portability may be diluted, reducing its utility as a tool for promoting competition and consumer empowerment. Adopting stricter technical requirements will ensure that the big players cannot erect non-transparency constraints that lock SMEs into their platform, giving the latter the same chances of competing.

Second, the GDPR example proves that subsequent regulation must control compliance costs impacting smaller companies. To prevent harm on SMEs, India could adopt graduated or proportional implementation of portability obligations where the stringency of the call may differ based on the size of the data processing by the entity and the control that may be exercisable mainly by large entities. However, India can help the SMEs develop the necessary infrastructure for making data portable, which will also help them in avoiding monopoly that is created around specific data sets without directly favoring large organizations.

Last, the GDPR's data portability provision is evidence of the need for ongoing supervision to protect against further consolidation of data by the major platforms. In this regard, India might allow its competition regulators to deal with and prevent cases where portability can cause the tendencies that harm market pluralism while portability mechanisms should enhance customer choice.

IV. PRIVACY-ENHANCING TECHNOLOGIES (PETS) AND ANTI-COMPETITIVE RISKS

A. PETs: Advancing Privacy but Restricting Market Access?

Encryption, Anonymity, and differential privacy which constitute PETs play an important role in fortifying the digital economy data protection. These technologies enable data to be processed while at the same time, preserving it from prying eyes; this means that it fulfils privacy requirements that would otherwise prevent data from being processed as required. It is most important in business sectors dealing with big volumes of consumers' information, including the finance,

medical and buying sectors, and make it possible for companies to develop trust with the customers since the data is more secure.[26] However, while PETs provide robust protections for individual privacy, they can also impose restrictions on data access that may have unintended consequences on market competition.

i. The Benefits of PETs for Data Privacy and Compliance

PETs work by minimizing the amount of data exposed during processing or by encrypting it in ways that protect against unauthorized access. For instance, encryption techniques can safeguard data at rest and in transit, ensuring only authorized parties can decrypt and interpret it.[27] Anonymization, on the other hand, removes identifiable details from datasets, reducing the risk of personal identification while allowing for data analysis. Differential privacy proposes noise addition, and data utility is generalized protecting individual data privacy. These methods are consistent with data protection laws across the world including India's pending DPDPA and European union's GDPR which embrace such favourable privacy oriented techniques.

The complexity of PETs increases the set of regulations that these companies must follow and the focus of consumers on the protection of their data makes companies investing in PETs have legal advantages in today's world. Further, compliance with the privacy laws not only minimises legal exposures but also alleviates the competitive advantage since consumers prefer firms with sound privacy policies. PETs can therefore become instrumental in determining market success by making companies meet both the regulatory provisions and customers' expectations on data protection.

ii. Balancing Privacy and Competition in PET Implementation

Thus, to introduce impartiality towards PETs negative effects on privacy and market fairness, certain strategies of regulation could be applied. International organisations, similar to India's Competition Commission, could look into the prospect of analysing frameworks that ensure the release of anonymised data at a huge level to smaller firms does not impinge privacy, without creating a revision. Furthermore, it is potential for policy interventions to provide SMEs equal opportunities in obtaining or developing PETs. For example, the creation of common facilities

[26] Hasani, T., Rezania, D., Levallet, N., O'Reilly, N. and Mohammadi, M., 2023. 'Privacy enhancing technology adoption and its impact on SMEs' performance'. *International Journal of Engineering Business Management*, *15*, p.18479790231172874.
[27] Information Commissioner's Offices, 'Privacy-enhancing technologies (PETs)'. <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf.>.

or consortium for Open Source PETs' development could help reduce costs which smaller firms had to bear so they could remain competitive while maintaining privacy legislation compliance.

B. Striking a Balance: PETs, Market Power, and Innovation

Privacy-Enhancing Technologies (PETs) have become crucial in today's digital economy, especially in managing user data responsibly. However, the implementation of PETs can paradoxically consolidate the market power of data-rich incumbents, potentially stifling innovation. In markets like India, where major tech firms are rapidly adopting these technologies, there is an increasing need for regulatory oversight to ensure that privacy-focused innovations do not inadvertently lead to anti-competitive outcomes.

i. Entrenching Market Position of Data-Rich Firms

PETs, such as advanced encryption, differential privacy, and anonymization techniques, serve as both data security tools and as compliance mechanisms for companies handling massive amounts of personal information. Most data-rich firms can afford the resources needed to roll out such technologies to achieve secure user data and satisfy the measures set by the data protection laws such as the DPDPA of India. Conversely, the SMEs or start-ups may experience some difficulties of financial and technical resources that would offer the same degree of PETs. This limitation can also prevent successful access to valuable user information and also restrain the competitive position against informational firms.

For instance, GPEs can use PETs to analyze big data to obtain more advanced insights into customer behavior while preserving their privacy, which large firms, often caught in the middle of restrictions and privacy breaches, can take advantage of. This ability gives them the opportunities to improve their service, create the targeted advertisement, and adjust the experience to the clients based on rather safe but rather descriptive data analysis.[28] On the other hand, the firms with less or no PET have limited ability of processing and analyzing the available information in the same way as the firms in the first group. As an unexpected outcome, PETs can enhance competitive protection for data-intensive organizations by restricting the access of new market entrants to data accumulation, processing, and analysis.

Moreover, the regulatory measures demanding higher levels of privacy and security inevitably contribute to these large firms' strategic profiles; the compliance costs associated with PETs are

[28] Arora A and Jain T, 'Data Sharing between Platform and Seller: An Analysis of Contracts, Privacy, and Regulation' (2024) 313 European Journal of Operational Research 1105.

unlikely to be manageable by entrants and other smaller players. For instance to conform to DPDPA firms have to put in place structures for privacy compliance that may entail purchase of higher level of encryption and anonymization. Such investments may be expensive for startups or SMEs which are under pressure on their constrained budgets and may hamper the innovation or consolidate the market for the benefit of large players.

ii. Regulatory Responses to Balance PETs and Competition

To avoid PETs becoming a means for the biggest firms to strengthen their grip on the market, which is already happening today, regulators must look for ways to promote more open access to privacy-enhancing technologies. The regulators can make equal opportunities in the competition by putting in place policies that ensure that both competitors who have strong PETs policy compliances and those who have weak ones are allowed into the market through regulating policies of PETs to compete fairly while at the same time protecting data privacy.

Some possible regulatory strategies will allow giving different financial rewards or subsidies to SMEs who use PETs. For example, the Indian government could offer grants for SMEs to help implement PET or tax incentives that would allow the firms to meet privacy needs using their scarce resources. Moreover, regulators may encourage suppliers of open-source PETs which many small firms may use to get relatively affordable privacy tools with comparable capabilities to those that major organizations employ.[29] Other benefits of open source collaborations are to also foster new inventive PETs to reach new players so as to avoid being dominated by the few firms with ample data.

The next regulation issue is the requirement of data-sharing systems that provide anonymity or aggregated databases to small firms. In such a case, data-intensive firms will have to disclose some of the categories of data responsibly in order to level the playing ground for SMEs. There is nothing wrong with having more actors within the food technology ecosystem benefit from anonymized datasets to make their analytics better, create competitive products, and innovate for the consumer's sake without the invasion of privacy. Such data sharing mechanisms would of course require supervision in order not to violate the rights of the users but they would certainly be useful in curbing competition in data oriented markets.

[29] Yanamala, A.K.Y., Suryadevara, S. and Kalli, V.D.R., 2024. 'Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence'. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), pp.1-43.

Another approach to a balanced approach could also be facilitated by a regulatory sandbox model. Through authorising firms particularly SMEs to experiment with PET applications under monitored conditions, the regulators will be in a position to gather facts on the effect of these technologies on privacy and competition. Loosened or flexible regulatory environments through sandboxes can encourage innovation through temporary waivers of legal and regulatory constraints for companies seeking new means of engaging PETs and a competitive tactical advantage without suffering the complete costs of compliance.

C. Case Study: PET Implementation in Indian Tech Firms

i. Examples of Indian Companies Leveraging PETs

This research identified that several Indian technology companies have started using PETs in their business model as they look to improve user data protection in the wake of new data protection laws. The present form of PETs is used by several firms that include Jio and Paytm in data handling practices, while firms such as Flipkart adopted more advanced forms of PETs such as FIP. For example, relaying to Jio; the organization has enhanced encryption processes on its platforms to secure users' information minimizing privacy issues while enhancing users' confidence. Paytm, the biggest digital payment company in India has adopted some anonymization strategies that help them to keep user data secure while at the same time getting significant information from the data garnered from many users.

Differential privacy has been adopted by Flipkart, the largest online shop in India, to understand consumer buying pattern discretely. Integrated in their processes, these technologies show that these firms are privacy-savvy and, at the same time, retention-savvy, which could be used as competitive advantage. These examples show how Incumbent firms are beginning to seek to improve customers' confidence through enhancing PETs and potentially deepen markets, thereby cementing themselves.[30]

ii. Impact on Consumer Trust and Market Dynamics

This paper also discussed some of the effects of the adoption of PETs by Indian tech companies concerning customer trust and the markets. Due to increased concerns regarding data privacy, when firms are using PETs to safeguard consumers' information, these firms are regarded highly

[30] Baum, C., Chiang, J.H.Y., David, B. and Frederiksen, T.K., 2023. Sok: Privacy-enhancing technologies in finance. *Cryptology ePrint Archive*.

in the market. This heightened consumer trust translates into increased user engagement, loyalty, and a competitive edge, particularly as data privacy awareness continues to grow in India.

However, this emphasis on PETs may also contribute to market concentration. As leading firms implement high-end privacy measures, they become more attractive to privacy-conscious consumers, which, in turn, reinforces their market dominance.[31] Consequently, smaller firms that lack comparable PET infrastructure find it challenging to compete, potentially leading to reduced market diversity and consumer choice.

V. CONSENT, MARKET POWER, AND REGULATORY CHALLENGES IN DATA-DRIVEN MARKETS

A. Defining Market Power in Data-Intensive Sectors

In data-driven markets, defining market power is complex due to the unique role that data plays in shaping competitive dynamics. Unlike traditional markets, where market power is largely based on economic parameters such as market share, revenue, or asset control, data-centric sectors require a more nuanced approach that considers the intangible yet influential value of data. The challenge in assessing market power lies in identifying how data accumulation translates into competitive dominance, particularly in Indian digital markets where companies leverage data to enhance services, personalize consumer experiences, and streamline operations.[32]

i. Challenges in Determining Relevant Markets

Market delineation in data-driven sectors is essential to assess whether a firm holds dominance, yet it presents unique complications. Traditional market definitions, which rely on product substitutability or geographic boundaries, often fall short in capturing the complex interplay of data. Digital platforms often operate in multi-sided markets—such as social media, e-commerce, and digital payment systems—where users and service providers interact simultaneously. For instance, companies like Paytm or Flipkart operate across multiple consumer categories (payments, shopping, etc.), where user data from one segment can be leveraged to influence consumer behaviour in others. In such cases, defining a single "relevant market" becomes challenging since

[31] Boteju, M., Ranbaduge, T., Vatsalan, D. and Arachchilage, N.A.G., 2023. SoK: Demystifying privacy enhancing technologies through the lens of software developers.
[32] Shukla, S., Bisht, K., Tiwari, K. and Bashir, S., 2023. The economy of data privacy. In *Data Economy in the Digital Age* (pp. 87-100). Singapore: Springer Nature Singapore.

data-driven products frequently extend across market boundaries and cater to interconnected consumer bases.

Moreover, data-intensity alters traditional consumer metrics. Unlike markets where consumer loyalty is price-driven, data-centric markets often exhibit "data network effects," where a product's value to each user increases as more users join and contribute data.[33] This effect is visible in the Indian context, where tech giants like Jio and Amazon India can gather vast data volumes from large user bases. These data troves allow companies to refine algorithms, predict consumer trends, and improve user experiences in ways smaller competitors cannot match. Hence, traditional methods of defining markets might misrepresent the competitive landscape in data-driven industries, where consumer value stems as much from data control as from conventional product offerings.

ii. Assessing Dominance Through Data Control

Once the market is delineated, determining dominance in data-driven sectors hinges on evaluating data control and its effects on competitive positioning. Unlike tangible assets, data is replicable and non-rivalrous, which makes concentration challenging to measure purely in quantitative terms. Indian regulators face the task of assessing how data control enables firms to exercise undue influence over markets, potentially stifling competition and innovation.

In India's digital economy, data-rich firms like Jio and Amazon India have been able to leverage their vast data resources to consolidate market power. Thus, analyzing behavioural patterns these companies adapt value propositions that are highly targeted and act as key barriers for new entrants who cannot gain similar levels of consumer understanding. This dynamic can help discourage other smaller competitors as well since they do not possess the same quantity and types of data that can be used to anticipate consumer behaviour or maximize service outcomes.

B. Consent as a Dual Factor in Privacy and Competition Regulation

i. Exploration of Consent Mechanisms in the DPDPA and Competition Act

Consent occupies similar significance in the Indian regulatory system operating as a legal tool in two contexts, in the DPDPA and in the Competition Act while functioning to preserve user self-governance and fostering fair market competition. The DPDPA focuses on the concept of

[33] Govindarajan and Venkatraman, (2024) 'Fusion Strategy: How Real-time Data and AI Will Power the Industrial Future', *Harvard Business Press.*

'consent' as the lawful means of processing data, and where data is being collected, it mandates that the use of the data must be disclosed. It requires organizations to give users meaningful information about how collected data will be used so that consumers can control their data. This approach is not unlike the user-focused approach found in worldwide data protection regulations reaffirming the user's right to decide who can use the information submitted by them and in what manner.[34]

In the Competition Act, however though, it may not be a direct player, consent has considerable implications. Competition law has evolved over the years with an emphasis on the efficient consumer surplus and what was previously a commercial risk analysis of possibly acting foreclosed, exclusionary or predatory that resulted in using consumer data to entrench market power. Over time, using this approach has shifted as the authorities begin to understand data gathering and applying it practices, even with user consent, can contribute to anti-competitive behaviour. If a dominant firm uses consented data to create personalized services that are unavailable to rivals due to data inaccessibility, this can create a de facto monopoly.[35] Thus, the Competition Commission of India (CCI) is increasingly examining data-centric consent mechanisms not only for privacy compliance but also for their potential to influence market dynamics.

ii. Interplay Between User Consent, Data Control, and Market Competition

User consent, while foundational to privacy, can also reinforce data control mechanisms that impact competition. Large tech companies that operate in India—such as Google, Facebook, and Amazon—often gather and process vast quantities of user data with consent, which they then use to refine their services and tailor them to individual preferences. This practice, while beneficial for user experience, can also limit consumer choice by solidifying the market positions of these firms. Therefore, the smaller competitors do not have similar data volumes, which become a cue to enter the market making its dynamism limited. In other words, consented data collection makes it possible for large firms to create bespoke service delivery mechanisms that competitors cannot imitate, through increased consumer devotion – thus a more fortified competitive advantage.

The DPDPA and the Competition Act must firstly coordinate on the impacts of various kinds of consents regarding the use of data. For example, under the DPDPA, consent operates mainly to prevent data misuse, while in the same sense and under competition law, the same consent makes

[34] Belli, L. and Doneda, D., 2023. 'Data protection in the BRICS countries: legal interoperability through innovative practices and convergence'. *International Data Privacy Law*, *13*(1), pp.1-24.
[35] Pathak, M., 2024. 'Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act' *(February 6, 2024)*.

a dominant firm gain exclusive information on consumer behaviour.[36] This is in light of the fact that current approach to consent fails to strike the right balance between protecting privacy while at the same time preventing players from being locked out of the market through these consent structures.

One bright idea is to regulate how the consented data can be used by the companies for the purpose of competing. To overcome the monopolistic control of the user data generated by these platforms, the Indian government ought to set certain regulations that enforce data portability or data interoperability. For example, if a user agrees to transmit data to a dominating firm, it may also have an opportunity to forward the same data to a rival, ensuring a more effective competitive setting.

C. Comparative Analysis with International Jurisdictions

i. Overview of the GDPR's Influence on EU Competition Policies

EU's General Data Protection Regulation (GDPR) have had a profound effect on the competition policies of the region and consequences relating to the interactions between privacy and competition law. GDPR also focuses on the rights of the data subjects, such as the right of access, right of portability and right to erasure, thus, enshrine data free movement which contributes to competition. I also know that thanks to data portability consumers for instance can freely switch between different service providers, thus reducing the switch cost, which fosters competition. This regulation targets the issue of market incorporation by the dominant digital platforms, and where privacy measures are also put and where it minimally or/and effectively protects the consumers, then it equally result in competitive market.[37]

Similarly, the European competition authorities have moved to increase pressure on data-driven monopolies especially with respect to search engines such as Google and Face book. The EC has looked at situations where strong firms use consumer data to lock out rivals, regarding the accumulation of data as one means through which firms achieve and exercise power over the marketplace. These investigations together with GDPR's pro-competition impacts illustrate how the privacy laws can be twin weapons in preserving fair competition.

[36] Modi, A. and Kesarani, V., 2023. 'Digital Lending Laws in India and Beyond: Scrutinizing the Regulatory Blind Spot'. *Indian Journal of Economics and Finance*, *3*(1), pp.1-7.
[37] Ucar, M. and Yalcintas, A., 2023. 'GDPR and Digital Protectionism in the EU: The Cases of Android and IOS'. *Journal of Economic Issues*, *57*(4), pp.1079-1094.

ii. Comparative Insights on Regulatory Approaches and Implications for Indian Policy

India can learn much from the EU's experience of GDPR and competition law. Although the concept of consent and data rights is already in the DPDPA, adding provisions that will speak to the proposed portability of data with restrictions on monopolistic data control can strengthen India's digital competition. If there were an express obligation to provide 'data portability', like the one observed in GDPR, it could help to increase entry by new smaller scale firms and, thereby assist in reducing the consumer lock-in that is at the heart of the two sets of concerns – privacy and competition. At the same time, the approach to interoperability mentioned in the GDPR may be useful in India to suggest to regulators; the ability of competitors to obtain the data they need, while not having an adverse impact on user privacy.

VI. CONCLUSION

Between data privacy rules, on the one hand, and competitive regulation, on the other, lie both threats and opportunities for India's digital economy. The Digital Personal Data Protection Act (DPDPA), while safeguarding personal information, also influences market dynamics, raising concerns about data monopolization and barriers for new entrants. The regulatory focus on data portability and consent highlights the complexities in balancing individual rights with competitive equity. However, privacy-enhancing technologies, though beneficial for consumer data protection, may inadvertently consolidate market power among established firms, limiting competition. Additionally, the difficulty in defining market power and assessing dominance within data-driven industries presents unique legal and regulatory challenges.

Comparative insights from the EU's GDPR illustrate that, while protective frameworks are essential, they must be designed to avoid reinforcing monopolies in digital markets. Case studies of Indian tech companies demonstrate the practical struggles in aligning with dual objectives of data protection and competition law, revealing a need for tailored policies that promote both consumer welfare and fair competition. Moving forward, India's regulatory approach should focus on fostering innovation while mitigating anti-competitive risks, ensuring a balanced framework that supports both data privacy and a dynamic, inclusive digital economy.