

SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases



ISSN NO. 2456-9704
Volume 10 Issue 3
www.supremoamicus.org



DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.



ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

**-Editorial Team
Supremo Amicus**



THE ROLE OF PERSONAL DATA IN ESTABLISHING MARKET POWER: COMPETITION LAW CHALLENGES IN THE AGE OF BIG TECH

By Astha Bhalavi

From National Law Institute University, Bhopal (NLIU)

By Akriti Goyal

From National Law Institute University, Bhopal (NLIU)

By Hitika Agrawal

From National Law Institute University, Bhopal (NLIU)

ABSTRACT

The digital economy has transformed personal data into a central source of market power, challenging the traditional foundations of competition law. This paper examines the growing intersection between data protection and competition law in India, focusing on how the dominance of Big Tech firms increasingly stems from control over data rather than from price. It analyses the Digital Personal Data Protection Act, 2023 (DPDPA) alongside the Competition Act, 2002, exploring how consent-based privacy frameworks may inadvertently entrench the position of data-rich incumbents while imposing disproportionate compliance costs on smaller players. The paper surveys the enforcement experience of the Competition Commission of India (CCI) in cases such as the Google Search Bias case, the WhatsApp privacy policy matter, and XYZ v. Alphabet Inc., and situates these within global developments including the European Union's Digital Markets Act and antitrust actions against Meta, Google, and Amazon. It identifies core doctrinal challenges confronting regulators — data as an essential facility, discriminatory access, cross-use of databases across markets, delineation of the relevant market, and self-preferencing — before proposing regulatory responses such as interoperability, data portability, institutional coordination, and an expanded consumer

welfare standard that looks beyond price. The paper concludes that effective regulation of Big Tech dominance in India requires a multidimensional, coordinated approach that treats data simultaneously as a personal right and a market asset.

Keywords: Big Data; Competition Law; Data Protection; Digital Personal Data Protection Act; Big Tech; Abuse of Dominance; Competition Commission of India; Digital Markets; Data Portability; Digital Competition Bill

INTRODUCTION

The core objectives of competition law preventing monopolies, promoting fair competition, and safeguarding consumer welfare are increasingly challenged by the dominance of Big Tech firms. These companies have not only transformed markets but also exposed the limitations of traditional legal frameworks designed for a pre-digital era. Their innovative business models, extensive reliance on data as a strategic asset, and global market presence complicate the effective enforcement of competition law in today's digital economy.

In today's digital era, information serves as a key economic resource driving innovation and shaping consumer experiences. Corporations increasingly depend on personal data to enhance services and engage customers, which has brought the intersection of data protection and competition law into sharp regulatory focus. In India, this convergence is most prominently reflected in the Digital Personal Data Protection Act (DPDPA), which seeks to safeguard personal information while addressing the challenges of a rapidly evolving digital marketplace.

Specialized data protection frameworks such as the DPDPA aim to enhance user autonomy through informed and proportionate consent in data processing. While this strengthens privacy, it may inadvertently entrench the dominance of major tech firms that already possess vast consumer datasets. These firms can more easily comply with regulatory demands, maintaining a competitive edge over smaller



players. Moreover, privacy-enhancing technologies, though intended to safeguard users, can further concentrate data control in the hands of established corporations. As data analytics and AI become central to competition, such dynamics risk limiting market entry, innovation, and consumer choice.

In this context, both established corporations and emerging technology start-ups depend extensively on gathering, processing, and strategically leveraging massive datasets to secure a competitive edge. Through the use of sophisticated computational tools, these entities convert large, fast-moving, and varied data into valuable insights with significant commercial potential—a process widely known as the utilization of Big Data. While the collection and use of personal data fall squarely within the scope of data protection regimes, antitrust authorities globally increasingly recognize that control over such data is a key indicator of market power. Consequently, access to and strategic exploitation of Big Data has become central to assessing whether dominant firms are abusing their market position, underscoring the growing intersection between data privacy and competition law in digital markets.

PERSONAL DATA AS A SOURCE OF MARKET POWER

The term ‘data’ lacks a singular, precise definition and is broadly understood to encompass information, facts, or statistics. In recent years, the concept of ‘Big Data’ has gained global attention, characterized by the four Vs: Volume, Velocity, Variety, and Veracity.¹ Big Data refers to vast amounts of diverse information collected, analyzed, and processed using advanced computational methods at high speeds to generate unique outcomes with commercial value. The collection, processing, and analysis of such data have become fundamental to modern marketing

strategies, enabling businesses to track market trends, understand consumer preferences, and optimize decision-making.

Digital technologies have exponentially expanded the capacity to gather and analyze large datasets, fueling the growth of the digital economy. Online service providers collect personal information directly via proprietary platforms such as websites and applications and indirectly by acquiring data from third parties, including social media platforms and search engines. By combining these sources, companies construct detailed individual profiles using advanced analytical techniques, often for targeted advertising, operational efficiency, and service personalization. Big Data also incorporates publicly available information, such as financial, geographic, and technical data, further enhancing the scope of insights derived.

Major technology and e-commerce firms, including Google, Amazon, Facebook, Apple, and Walmart, increasingly rely on Big Data analytics to influence consumer behavior, optimize services, and innovate.² Unlike traditional resources, data is non-rivalrous—it can be duplicated, reused, and repurposed indefinitely—allowing firms to continuously expand operations without limitation. Each user interaction—searches, purchases, or social media engagement—generates data that feeds machine learning systems, further improving services and attracting more users. This creates a “data advantage,” enabling companies with extensive datasets to innovate faster, utilize AI more effectively, and make informed business decisions compared to competitors with limited access.

In contemporary platform-based business models, the strategic use of data serves as a key competitive

¹ Pratyush Prakarsh and Harsh Vardhan, *Competition Law in the Age of Big Tech: Issues and Perspectives*, *International Journal for Multidisciplinary Research*, Vol 6 Issue 6, November – December 2024 <<https://www.ijfmr.com/papers/2024/6/28267.pdf>> accessed on 8th October 2025.

² Rishita Maheshwari, *The Intersection of Data Privacy and Competition Law: Analyzing Big Tech’s Market Dominance*, SSRN Papers, 14th May 2025 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5214841> accessed on 8th October 2025



differentiator. Platforms leverage data to develop personalized products and services, provide targeted advertising, and enhance engagement, which in turn strengthens lock-in effects and increases switching costs.³ For example, Google uses search data to deliver precise results and targeted ads, Facebook aggregates user behavior across Instagram and WhatsApp for advertising insights, and Amazon uses consumer data to optimize services and develop market-aligned products. The limited trading of datasets and proprietary control over analytics restricts traditional supply-demand assessments and reinforces market dominance.

In 2019, Germany's Federal Cartel Office ruled that Facebook abused its dominant position by forcing users to consent to extensive data collection, violating GDPR and constituting exploitative behavior under competition law. This case marked a global precedent linking privacy breaches with antitrust concerns. Similarly, the European Commission scrutinized Google for using personal data in ways that limited interoperability and hindered competition. Regulators in the UK and Australia are exploring measures like data portability and fair access to enhance competition, highlighting the overlap between privacy and market power.

The Facebook case, following its 2014 WhatsApp acquisition, was initially suspended by the Düsseldorf Regional Court but reinstated by the German Federal Court of Justice in 2020. The court emphasized that dominance can arise through non-price factors—like privacy and consumer autonomy—underscoring the close connection between data protection and competition law in digital markets.

From a competition law perspective, the concentration of personal data among dominant platforms raises significant concerns. Data can become a de facto barrier to entry, as possession of large datasets reinforces market power and may create monopolistic conditions.⁴ Practices such as exclusive data usage, limited sharing, or platform-specific analytics can reduce consumer choice and hinder the growth of new competitors. Furthermore, the intersection with data privacy issues compounds these concerns, as users often have limited understanding or control over how their data is collected, shared, or processed. Dominant companies can enforce stringent privacy terms that simultaneously protect their competitive position and exploit users, highlighting the critical need to evaluate data-driven market power within the frameworks of both competition and data protection laws.

DATA AND MARKET POWER: THEORETICAL LINKAGES

Competition law in India is grounded in neo-classical and harm theories, both prioritizing consumer welfare by preserving competitive markets. The rise of digital platforms has introduced new challenges, particularly concerning big data.⁵ By collecting, processing, and leveraging vast amounts of personal data, tech giants gain significant control over markets, raising the question of whether the exploitation of user data constitutes not only a privacy breach but also a misuse of market power. Platforms operating on multi-sided models monetize user data, creating entry barriers and anti-competitive concerns. While the CCI has not formally recognized data as a separate relevant market, it has expressed concern regarding access to data in notable cases such as Facebook's and Google's

³ Dr. Mahipal Lather, *Data as a source of market power: Competition law challenges in the age of AI and Big Data*, International Journal of Law, Volume 11, Issue 9, 2025, Page No. 19-23, 13-09-2025, <<https://www.lawjournals.org/assets/archives/2025/vol11issue9/11200.pdf>> accessed on 9th October 2025

⁴ Rupal Nayal, *Data Privacy at the Altar of Competition Laws*, Journal on Competition Law and Policy, Vol. 3, December 2022, pp. 79-95 <CCI+-

+2022+-+2023_Color-95-111.pdf> accessed on 9th October 2025.

⁵ Mayank Gandhi, *Big Data and Privacy in Digital Market: A Future Roadmap for Indian Antitrust Authority*, NLIU Law Review, Vol XII, Issue I, 2023 <<https://nliulawreview.nliu.ac.in/wp-content/uploads/2023/07/132-154-Vol-XII-Issue-I.pdf>> accessed on 9th October 2025



acquisitions of stakes in Jio, and Google's investment in Bharti Airtel.⁶

To determine a relevant market, the CCI considers both product and geographical boundaries, guided by supply and demand dynamics. On digital platforms, users provide data in exchange for "free" services, which is then analyzed and monetized either through advertising or sale to third parties. This establishes a clear demand-supply relationship, potentially justifying the classification of data as a separate relevant market. However, challenges arise: users do not receive monetary compensation, platforms' control over data is not exclusive, and a single platform's data may represent only a small portion of the overall market, limiting claims of market power. Despite their different origins, data-driven markets and complex digital ecosystems increasingly intersect with competition and data privacy policy, influencing economic activity and firm conduct. Digital ecosystems rely on personal data as a core business model and source of market power, sometimes blurring boundaries between the jurisdictions of competition authorities and data protection regulators. For instance, in the ad tech sector, EU data protection authorities examine lawful data processing for personalized services, while competition authorities consider whether privacy quality indicates abuse of dominance⁷. Models like "pay or consent" illustrate these overlaps, involving network effects, user lock-in, and pricing considerations, highlighting the need for regulatory collaboration.

The enormous market capitalizations of ecosystem giants such as GAFAM—Apple, Alphabet (Google), Microsoft, Amazon, and Facebook—reflect their substantial market potential and influence.⁸ These companies have displaced traditional industrial and financial leaders, consolidating their positions with valuations exceeding \$1 trillion post-COVID-19. The current capital market environment, with low interest rates and abundant liquidity, has enabled rapid investment in high-growth digital ventures, allowing newcomers to disrupt incumbents and attract funding from established firms.

By prioritizing growth over immediate profitability, these companies leverage software-driven production, characterized by high fixed costs and minimal replication costs, creating conditions for market dominance.⁹ The interplay of globalization, digitalization, economies of scope, and learning from consumer data further expands the notion of the relevant market, enabling firms to deploy data across multiple applications and strengthen their market power.

CONSENT DESIGN, "DARK PATTERNS" AND COMPETITION LAW CONCERNS

A growing body of regulatory attention has turned to the *design* of consent interfaces, rather than merely the substance of what is consented to. "Dark patterns" — interface choices engineered to nudge users toward broader data sharing, such as pre-ticked consent boxes, asymmetric choice architecture (a prominent "Accept All" button against a barely visible "Manage

⁶ Manu Goswami, Data Privacy vs. Market Power: Navigating the Intersection of Personal Information Protection and Competition Law in India's Digital Economy, Indian Competition Law Review, Vol. 9, Issue 2, <<http://iclr.in/wp-content/uploads/2024/12/ICLR-Vol-9-Issue-2-Article-4.pdf>> accessed on 9th October 2025.

⁷ Carolina Abate, Giuseppe Bianco, Francesca Casalini, *The Intersection Between Competition and Data Privacy*, OECD Roundtables on Competition Policy Papers, No. 310 <<https://doi.org/10.1787/20758677>> accessed on 10th October 2025.

⁸ Jay Modrall, *Antitrust risks and Big Data* Norton Rose Fulbright (June 2017) <<https://www.nortonrosefulbright.com/en-in/knowledge/publications/64c13505/antitrust-risks-and-big-data>> accessed 10th October 2025

⁹ Kolawole Afuwape, *Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces*, Journal of Digital Technologies and Law, 2024, 2(4) <<https://pure.jgu.edu.in/id/eprint/8973/1/Legal%20Aspects%20of%20Personal%20Data%20and%20the%20Issues%20of%20Competition%20in%20Digital%20Marketplaces.pdf>> accessed on 10th October 2025.



Preferences" link), or repeated consent prompts that wear down user resistance — sit at the intersection of the DPDPA's requirement of "free, specific, informed and unambiguous" consent and the Competition Act's prohibition on unfair conditions imposed by a dominant enterprise.

From a data protection standpoint, such designs may render consent legally defective, since genuine autonomy requires a real and easy choice to withhold data. From a competition standpoint, the same conduct can be characterised as exploitative abuse under Section 4(2)(a) where a dominant platform uses its market position to impose data-sharing terms that users would not accept in a genuinely competitive market. The German Facebook case is instructive here: the Bundeskartellamt treated Facebook's take-it-or-leave-it data terms as a form of exploitative abuse precisely because the absence of viable alternatives left users unable to exercise meaningful choice collapsing the usual distinction between a "privacy harm" and a "competition harm."

The difficulty for regulators lies in developing an objective standard for what counts as manipulative design, given that virtually all consent interfaces involve some degree of persuasive framing. A workable approach may involve looking at symmetry of choice (whether accepting and declining require equal effort), the presence of default options that favour data sharing, and whether the platform's dominance forecloses any reasonable alternative for the user. Regulatory guidance whether issued jointly by the CCI and the Data Protection Board, or through amendments to the CCI's abuse-of-dominance framework could usefully specify that consent-interface design constitutes conduct reviewable under Section 4 where it is deployed by a dominant enterprise to entrench a data advantage, rather than treating it as a matter for data protection law alone. Without such clarity, platforms retain an incentive to use design choices to extract broader consent than users would otherwise give, with the resulting data advantage compounding, rather than being checked by, existing dominance.

SECTORAL REGULATORY OVERLAP: RBI, TRAI AND SEBI IN DATA-DRIVEN DIGITAL MARKETS

Big Tech's expansion into regulated sectors digital payments, telecommunications-adjacent services, and financial products means that data-driven competition concerns increasingly arise within the jurisdiction of sectoral regulators such as the Reserve Bank of India (RBI), the Telecom Regulatory Authority of India (TRAI), and the Securities and Exchange Board of India (SEBI), alongside the CCI. A platform's use of transaction data gathered through a payments product to cross-subsidise or promote its core business, for instance, implicates RBI's data localisation and payment-system regulations as much as it does Section 4(2)(a) of the Competition Act on leveraging dominance across markets.

This creates a layered regulatory landscape in which the same conduct such as WhatsApp Pay's integration within WhatsApp, examined by the CCI in *Harshita Chawla v. WhatsApp Inc.* could equally attract RBI scrutiny under payment-system authorisation norms, or TRAI oversight where bundled telecom and app-based services are involved. Sectoral regulators typically possess deeper technical knowledge of their industries and a mandate for prudential or systemic-stability concerns, but comparatively limited experience assessing market-wide competitive effects, which remain the CCI's core institutional expertise. Divergent regulatory philosophies can also produce inconsistent outcomes: a data-sharing arrangement that a sectoral regulator approves for consumer-protection or interoperability reasons might independently raise dominance concerns before the CCI, and vice versa.

International experience offers a partial template: the UK's Digital Regulation Cooperation Forum extends beyond competition and data authorities to include sector regulators such as Ofcom and the Financial Conduct Authority, precisely because digital conduct increasingly cuts across traditional regulatory silos. India lacks an equivalent standing mechanism, though ad hoc coordination has occurred for instance, RBI's



separate scrutiny of payment aggregators alongside CCI's competition review of the same entities. A formalised framework for the CCI to consult, and be consulted by, sectoral regulators before finalising positions on data-driven conduct in regulated markets would reduce the risk of conflicting orders, allow the CCI to draw on sector-specific technical expertise, and ensure that data-driven dominance concerns are not overlooked simply because the underlying product also falls within a sectoral regulator's mandate.

DATA-SHARING MANDATES AND OPEN DIGITAL INFRASTRUCTURE AS PRO-COMPETITIVE TOOLS

Beyond prohibitory rules against data hoarding and self-preferencing, India has begun experimenting with an affirmative regulatory strategy: building shared digital infrastructure that structurally limits the ability of any single platform to monopolise data. The Account Aggregator framework, developed under RBI's oversight, allows individuals to consolidate and portably share their financial data across banks, lenders, and fintech platforms through a consent-based architecture, rather than leaving that data siloed within whichever institution first collected it. Similarly, the Open Network for Digital Commerce (ONDC) seeks to "unbundle" e-commerce by separating buyer-side and seller-side applications from the underlying transaction and discovery layer, so that no single dominant platform controls the data generated by a transaction end-to-end. The Unified Payments Interface (UPI) offers an earlier and now well-established precedent for this model, having prevented any single payments app from monopolising transaction data by mandating a common, interoperable rail that any licensed player can plug into.

These initiatives represent a structural alternative to the conduct-based remedies typically pursued under Section 4 of the Competition Act. Rather than waiting for a dominant firm to abuse a data advantage and then prosecuting that abuse after the fact, open infrastructure aims to prevent the data advantage from consolidating into unassailable dominance in the first

place, by design. This mirrors and in some respects goes further than the EU's DMA interoperability mandates, which impose portability and access obligations only on already-designated gatekeepers, whereas India's approach builds openness into the market's foundational architecture regardless of any individual firm's size.

However, such infrastructure is not without competition risk of its own. The design choices embedded in shared infrastructure — governance rules, technical standards, API access terms, and default settings — can themselves become sites of capture by well-resourced incumbents who are best placed to shape standard-setting processes to their advantage, participate earliest, or dominate the "unbundled" layers despite the underlying architecture being formally neutral. A large existing player joining an open network may still out-compete smaller entrants on the strength of pre-existing brand recognition, capital, and user trust, even where the data layer itself is shared. There is also a risk that mandatory data-sharing infrastructure, if poorly designed or under-resourced in its governance, could itself become a new single point of failure, a target for security vulnerabilities, or a de facto technical standard that stifles competing innovation in data architecture by locking the ecosystem into one approach prematurely.

For competition law, the emergence of shared digital infrastructure raises novel questions that existing doctrine has not yet resolved: whether meaningful participation in such infrastructure should be treated as a factor reducing a finding of dominance under Section 4, whether governance capture of shared infrastructure by incumbents should itself be assessed as an abuse, and how the CCI should coordinate with the sectoral bodies overseeing these initiatives — RBI for Account Aggregators, the Department for Promotion of Industry and Internal Trade for ONDC, and the National Payments Corporation of India for UPI — to ensure that open infrastructure delivers genuine contestability rather than merely relocating



dominance to a new layer of the stack, such as the app layer built atop an otherwise open network.

DUE PROCESS AND JUDICIAL REVIEW CONCERNS IN EX-ANTE DIGITAL REGULATION

The shift toward ex-ante regulation, exemplified by India's proposed Digital Competition Bill and its "Systemically Significant Digital Enterprise" (SSDE) designation, raises administrative and constitutional law concerns distinct from those under the existing conduct-based framework of the Competition Act. Under Section 4, a finding of abuse of dominance follows a fact-specific inquiry, with the enterprise given an opportunity to contest both the market definition and the alleged conduct before the CCI, and subsequently before the National Company Law Appellate Tribunal and the Supreme Court, allowing the underlying economic and factual premises to be tested through adversarial process. Ex-ante designation, by contrast, typically applies a fixed list of obligations automatically upon an enterprise crossing quantitative thresholds — such as turnover, user numbers, or market capitalisation — with comparatively limited scope to contest the underlying premise that the designated conduct is, in fact, anti-competitive in that firm's specific case, since the obligations attach by category rather than by proven harm.

This raises two connected due-process concerns. First, principles of natural justice require that an enterprise facing significant behavioural obligations have a meaningful opportunity to be heard before designation, not merely a right to seek review afterward; the Digital Competition Bill's drafting has drawn criticism for the limited pre-designation hearing it contemplates compared to the EU's DMA, which itself has faced litigation from designated gatekeepers such as Apple, Meta, and ByteDance contesting the scope, timing, and object of their obligations before the EU courts, illustrating that even a mature ex-ante regime generates substantial contestation over designation criteria. Second, the fixed and largely irrebuttable nature of ex-ante

obligations sits uneasily with the proportionality standard that Indian administrative and constitutional law ordinarily demands of regulatory measures restricting a party's commercial freedom under Article 19(1)(g) of the Constitution, which typically requires that restrictions be the least restrictive means of achieving a legitimate regulatory aim rather than a blanket, threshold-triggered obligation applied uniformly across designated enterprises regardless of their individual conduct.

A further concern is the risk of regulatory overreach through vague or overly broad thresholds that sweep in enterprises whose specific conduct does not, in fact, raise competition concerns, effectively presuming anti-competitive risk from scale alone rather than from demonstrable harm. This is compounded by the pace of digital market evolution: a firm designated as systemically significant today may lose that position within a few years as market structures shift, yet a static designation process risks leaving obligations in place well after the underlying justification has disappeared, imposing ongoing compliance costs without a corresponding competitive benefit. Comparative experience suggests that workable ex-ante frameworks need calibrated, evidence-based designation criteria, a genuine pre-designation consultation process, a defined and time-bound right of appeal on both procedural and substantive grounds, and periodic review mechanisms allowing designation to be revisited as a firm's market position evolves safeguards that Indian legislators will need to build into the Digital Competition Bill if it is to withstand constitutional scrutiny while still delivering the enforcement certainty that ex-ante regulation promises.

CORE CHALLENGES IN ENFORCING COMPETITION LAW IN BIG TECH

Enforcing competition law against Big Tech presents significant challenges due to the distinctive features of digital markets, the complex business models of these firms, and their global operational scope. The following sections examine the key issues that



regulators encounter when seeking to apply traditional competition rules to these technology giants.

1. Refusal to Grant Access to Data: A major antitrust concern surrounding Big Data is that large corporations may use their data dominance to block new or smaller firms from entering the market. By leveraging data analytics to study user behavior and deliver targeted advertising, established firms gain a significant competitive advantage in data-driven markets. Smaller players, lacking comparable datasets and advanced analytical technologies, struggle to compete effectively, making Big Data a potential entry barrier.

The European Court of Justice has held that a data-rich dominant enterprise generally cannot be compelled to share its data with competitors, except in exceptional circumstances where the data constitutes an essential facility—that is, indispensable and unavailable through any alternative means. While some argue data is inherently non-exclusive, the real barrier lies in the ability to process and derive insights from vast and complex datasets.

The *Microsoft v. Commission*¹⁰ case is illustrative: Microsoft's refusal to share interoperability information with Sun Microsystems was deemed anti-competitive, as it prevented effective competition. Similarly, refusal by a data-dominant firm to share essential datasets could restrict market access and eliminate competition. Under Section 4(2)(c) of the Competition Act, 2002, such conduct amounts to abuse of dominance through denial of market access and foreclosure of competition.

2. Discriminatory Access to Data: Discriminatory sharing of data is another concern, particularly visible in the e-commerce sector. The European

Commission has accused Amazon of misusing data collected from third-party sellers to strengthen its downstream operations. Amazon's affiliates benefit from exclusive access to recent and relevant consumer data, enabling them to design cost-effective products and target consumers more efficiently than non-affiliated competitors.¹¹ Since Amazon's proprietary data is unique and cannot be easily replicated or purchased, competitors face high entry costs, limiting their ability to compete. Such conduct may amount to foreclosure of competition in downstream markets. Under Sections 4(2)(b) and 4(2)(c) of the Competition Act, discrimination in access to essential data constitutes an abuse of dominant position by imposing unfair or discriminatory conditions in the sale or provision of services.

3. Cross-Use of Databases: Data-dominant firms may exploit data collected in one market to enhance or extend their dominance into another, leading to potential market foreclosure. Under Section 4(2)(e) of the Competition Act, using dominance in one relevant market to enter or protect a position in another amounts to abuse of dominance.

Such practices often take the form of tying or bundling, where a dominant firm links access to its datasets with other products or services, compelling consumers to purchase both. The Competition and Markets Authority (CMA) has highlighted how data-rich entities can leverage their vast databases to dominate related markets, such as analytical services.¹² While such integration can yield efficiencies, it also deters new entrants and reduces competition. Thus, leveraging data assets across markets may

¹⁰ *Microsoft Corp. v Commission* (2007) T-201/04

¹¹ Bruno Lasserre and Andreas Mundt, *Competition law and Big Data: The Enforcers' View* (Bundeskartellamt, 2017) <<https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Fachartikel/Compet>> accessed 10th October 2025.

¹² Daniel Mandrescu, *Tying and bundling by online platforms – Distinguishing between lawful expansion strategies and anti-competitive practices* (2021) 40 Computer Law & Security Review, <<https://www.sciencedirect.com/science/article/pii/S0267364920301047?via%3Dihub>> accessed 02 March 2022.



constitute an abuse under Section 4(2)(e) of the Act.

4. **Delineating Relevant market:** Digital markets evolve rapidly and differ from traditional markets, featuring zero-price segments, network effects, and winner-takes-all dynamics that can lead to user lock-in. Big Data and analytics are central to competition, while multi-sided platforms connect diverse user groups, creating direct and indirect network effects. The rise of digital ecosystems and conglomerates further reduces competition.¹³ Online and offline channels raise questions about market boundaries, and data-for-service models challenge traditional market definitions. Evaluating platform sides separately may oversimplify, while treating the entire platform as one market can be too broad, requiring a rethink of conventional approaches in competition law.
5. **Self-preferencing:** Tech giants often secure prominent placement for their products in online searches, increasing consumer preference through visual prominence. Self-preferencing also includes restricting competitors' marketing access, replicating rivals' strategies ("sherlocking"), and using default settings to steer users toward their products. These practices raise rivals' costs, forcing them to rely on costlier advertising alternatives. For instance, Apple faced a complaint from Spotify over such practices, leading to ongoing legal proceedings before the European Commission (EC). In India, the Competition Commission of India (CCI) encountered a comparable issue in *XYZ v. Alphabet Inc. and Ors*¹⁴, where it directed a comprehensive investigation into Google's alleged abuse of dominant position particularly concerning the preferential treatment and

placement of Google Pay on the Google Play Store.

CCI AND ISSUES INVOLVING DOMINANCE IN THE DIGITAL ERA

Dominance in itself is not prohibited under competition law; it is the abuse of such dominance that attracts liability. The Competition Commission of India (CCI) follows a two-step test to determine: (1) whether an enterprise holds a dominant position in the *relevant market*, and (2) whether it has *abused* that position.¹⁵ With the rise of digital platforms, challenges surrounding dominance have intensified, especially in technology and data-driven markets.

In the Google Search Bias Case, CCI found Google guilty of abusing its dominance by displaying irrelevant ads and imposing unfair conditions on advertisers, violating Section 4(2)(a)(i) of the Competition Act. Subsequent investigations in 2019 and 2020 also found Google abusing its position through mandatory pre-installation of Google Mobile Services and preferential promotion of its payments app, respectively, echoing similar findings by the EU. In the WhatsApp case, informant Vinod Kumar Gupta alleged that WhatsApp's 2016 privacy policy—mandating data sharing with Facebook—constituted an abuse of dominance and predatory pricing. While CCI initially dismissed the case citing users' ability to opt out, it later, in 2021, took suo motu cognizance when WhatsApp removed this opt-out option, creating a "lock-in" effect for users. The Delhi High Court upheld CCI's jurisdiction to investigate despite pending related matters before the Supreme Court.

In *Meru Travel Solutions Pvt. Ltd. v. Uber India Systems Pvt. Ltd.*,¹⁶ CCI examined allegations of predatory pricing in a data-driven platform economy.

¹³ Shubha Ojha, *Tackling Big Tech's Data Advantage: Is the Indian Regulatory Framework Geared Up?*, Indian Competition Law Review, Volume 6(2), November 2021, pp 55-73, <<http://iclr.in/wp-content/uploads/2024/03/ICLR-Volume-62-Article-5-pp-55-73.pdf>> accessed on 11th October 2025.

¹⁴ Case No. 07 of 2020.

¹⁵ Eshita Gupta and Yagya Agarwal, *Big Data Dominance: Underpinning the Separate Relevant Market*, SSC Online Blog, August 23, 2024, <<https://www.sconline.com/blog/post/2024/08/23/big-data-dominance-underpinning-the-separate-relevant-market/>> accessed on 11th October 2025.

¹⁶ Appeal No. 31 of 2016.



Though the case primarily dealt with pricing and market dominance, it highlighted how data-enabled network effects where increased users strengthen a platform's position—can create market power. CCI ultimately found Uber not dominant, recognising that competitive pricing and data-driven growth strategies alone do not amount to abuse under Section 4.

In *XYZ v. Alphabet Inc. (2020)*,¹⁷ the CCI directly confronted data-related concerns. The informant alleged that Google used its dominance in the Android OS and Play Store markets to promote Google Pay through pre-installation, preferential placement, and exclusive use of Google's payment system. Here, CCI acknowledged the role of data integration and platform control as potential tools for exclusionary abuse, forming a prima facie view of violation and directing an investigation under Section 26(1).

By contrast, in *Satyen Narendra Bajaj v. PayU Payments Pvt. Ltd.*¹⁸ and *Harshita Chawla v. WhatsApp Inc.*¹⁹, the CCI emphasised that dominance and data advantage alone do not establish abuse. In the WhatsApp Pay case, the Commission held that automatic installation of the payment feature within a widely used messaging app did not amount to anti-competitive conduct, as mere access to user data or presence on devices does not ensure consumer lock-in or usage.

CROSS-BORDER ENFORCEMENT AND INTERNATIONAL REGULATORY COOPERATION

Big Tech's global operations mean that a single data-driven practice a consent design, a self-preferencing default, or a data-sharing arrangement is typically deployed simultaneously across dozens of jurisdictions, while enforcement remains fragmented along national lines. This creates practical challenges for the CCI in at least three respects. First, evidence gathering is complicated where relevant data, source code, or corporate decision-making occurs outside

India, requiring reliance on mutual legal assistance mechanisms or voluntary cooperation from foreign parent entities that may be slower and less complete than domestic investigations. Second, remedies ordered by the CCI apply only within India, meaning a global platform may continue an identical practice in other markets even after an adverse finding here, unless the remedy is specifically designed to alter the platform's global architecture. Third, diverging outcomes across jurisdictions for instance, a practice cleared by one competition authority but found abusive by another, as has occurred with aspects of Google's conduct across the EU, US, and India create uncertainty for both regulators and regulated firms about the applicable global standard.

International cooperation mechanisms, such as the International Competition Network and bilateral cooperation agreements between the CCI and foreign authorities, provide informal channels for information exchange and coordinated timing of investigations, but stop short of mutual recognition of findings or joint remedial action. The EU's DMA, by contrast, achieves a degree of cross-border consistency simply by virtue of its scale a gatekeeper's EU-wide obligations often influence its global product design, producing a "Brussels effect" that indirectly benefits other jurisdictions, including India, without those jurisdictions needing equivalent regulatory capacity of their own.

For India, strengthening cross-border enforcement capacity would involve deepening formal cooperation agreements with major counterpart regulators (the European Commission, the US FTC and DOJ, and the UK CMA) to enable more systematic evidence-sharing and coordinated investigation timing, while remaining alert to the risk that over-reliance on foreign regulatory findings could compromise the CCI's independent assessment of India-specific market conditions, which often differ materially from those in more mature digital markets.

¹⁷ Case No. 07 of 2020.

¹⁸ Case No. 23 of 2019

¹⁹ Case No. 15 of 2020



MERGER CONTROL AND "KILLER ACQUISITIONS" OF DATA-RICH START-UPS

A distinct enforcement challenge arises not from established dominance but from acquisitions that pre-empt future competition before it materialises. Dominant technology firms frequently acquire nascent start-ups holding valuable datasets, novel algorithms, or promising user bases — not necessarily to integrate their technology, but to neutralise a potential future rival or absorb a complementary data asset that strengthens the acquirer's existing ecosystem. Because such start-ups typically generate limited revenue or turnover at the time of acquisition, these transactions have historically fallen below the asset- and turnover-based thresholds that trigger mandatory notification to the CCI under Section 5 of the Competition Act, allowing "killer acquisitions" to proceed without scrutiny of their long-term competitive effects.

The Competition (Amendment) Act, 2023 addresses this gap by introducing a deal-value threshold transactions exceeding ₹2,000 crore involving a target with substantial business operations in India now require notification irrespective of the target's turnover or asset value. This shifts the CCI's focus from a static, revenue-based test toward one capable of capturing acquisitions of data-rich but pre-revenue entities, aligning India's framework more closely with Germany's transaction-value threshold introduced after the Facebook–WhatsApp merger review gap became apparent globally.

However, deal-value thresholds alone do not resolve the substantive difficulty of assessing harm in these cases: traditional merger review tools, built around market share and price effects, are poorly suited to evaluating whether an acquisition eliminates a nascent competitive threat whose value lies in data, talent, or technological trajectory rather than current market presence. The CCI's institutional capacity to conduct such forward-looking, counterfactual analysis — asking not "does this reduce competition today" but "does this foreclose competition that would otherwise have emerged" remains underdeveloped. Comparative

practice from the European Commission's approach to "reportable but not notifiable" acquisitions, and academic proposals for a rebuttable presumption of harm where an incumbent acquires a start-up operating in an adjacent data market, offer potential models. Strengthening the CCI's specialised merger-review capacity for data-driven acquisitions is therefore a necessary complement to the deal-value threshold reform, since a notification requirement without the corresponding analytical capacity to interrogate the transaction achieves only partial protection against pre-emptive consolidation of data advantages.

ALGORITHMIC PRICING AND TACIT COLLUSION IN DATA-DRIVEN MARKETS

The increasing use of pricing algorithms by platforms and their affiliated sellers introduces a further complication for competition enforcement that intersects directly with data control. Where multiple firms deploy algorithms trained on shared or similar datasets including data licensed from a common dominant platform pricing outcomes may converge without any explicit communication or agreement between the firms concerned, a phenomenon often termed "tacit algorithmic collusion." This poses a doctrinal difficulty for Section 3 of the Competition Act, which is premised on establishing an "agreement" between enterprises; algorithms that independently learn to sustain supra-competitive prices through repeated interaction may produce collusive outcomes without any conduct that fits traditional notions of concerted action.

The concern is amplified where a dominant platform itself supplies the pricing algorithm or the underlying data to competing sellers on its marketplace, as has been alleged in various jurisdictions regarding platform-recommended pricing tools. In such cases, the platform's data control does not merely confer an advantage to itself but potentially facilitates coordination among ostensibly independent third parties, raising the question of whether the platform can be held liable as a facilitator of collusion under Section 3, even where it is not a direct party to the



resulting price alignment. The CCI has not yet directly addressed this fact pattern, though comparable concerns have been examined by the European Commission in the context of RPM-adjacent conduct involving algorithmic repricing tools.

Detecting and proving algorithmic collusion also strains conventional evidentiary approaches, since the relevant "agreement" may exist only in the parallel training and deployment of similar code rather than in any documented communication. This reinforces the need raised elsewhere in this paper for the CCI to develop dedicated technical and data-science capacity capable of auditing algorithmic conduct, including the ability to examine training data provenance, model design choices, and platform-supplied recommendation tools, rather than relying solely on traditional documentary evidence of coordination when assessing whether Section 3 has been contravened in increasingly automated digital markets.

STRUCTURAL VERSUS BEHAVIOURAL REMEDIES IN DATA-DRIVEN ABUSE CASES

Once an abuse of dominance rooted in data advantage is established, the CCI's choice of remedy raises questions that existing Indian jurisprudence has only begun to confront. Section 27 of the Competition Act empowers the CCI to impose behavioural remedies such as cease-and-desist orders, modification of conduct, or the discontinuation of specific practices like preferential placement or exclusive data-sharing arrangements as well as, in principle, more structural interventions. In practice, the CCI's orders to date, including those in the Google Android and Google Play Store matters, have been overwhelmingly behavioural: mandating changes to default settings, prohibiting anti-steering provisions, or requiring equal access to APIs, rather than compelling divestiture of data assets or business units.

Behavioural remedies offer the advantage of proportionality and administrative feasibility they target the specific conduct found abusive without disturbing the firm's broader corporate structure but

they carry a recognised weakness in data-driven markets: a dominant firm's accumulated data advantage, once built, persists even after the offending conduct ceases, meaning behavioural remedies may curb future abuse without disgorging the pre-existing advantage that conduct helped create. This is compounded by monitoring difficulty, since compliance with behavioural orders in algorithmic and data-driven contexts requires the CCI to verify conduct embedded in code and data-processing systems that are far less transparent than conventional pricing or output decisions, raising the same technical-capacity concerns discussed earlier in this paper regarding algorithmic auditing.

Structural remedies such as mandated data-sharing with competitors, enforced interoperability, or, in extreme cases, divestiture of a data-generating business line — more directly address the root cause of entrenchment but sit uneasily with the proportionality standard under Article 19(1)(g) discussed earlier in the context of ex-ante regulation, and have rarely been attempted globally outside exceptional cases. The EU's DMA effectively achieves a structural-remedy outcome through ex-ante interoperability and data-portability mandates imposed at the point of designation, rather than through post-hoc adjudicated remedies, suggesting that the structural-behavioural distinction may be less about remedy design in individual cases and more about whether a jurisdiction addresses data entrenchment through case-by-case enforcement or systemic ex-ante obligation. For India, a calibrated middle path behavioural remedies for isolated conduct, escalating toward mandated data-sharing or interoperability obligations where repeat or systemic abuse is found may offer a more workable framework than a binary choice between the two remedy types, and would benefit from explicit CCI guidance on the criteria governing that escalation.



DATA LOCALISATION AND CROSS-BORDER DATA FLOWS: COMPETITION IMPLICATIONS

Data localisation requirements — mandating that certain categories of personal or sensitive data be stored, and in some cases processed, within national borders — have emerged as a parallel regulatory instrument alongside the DPDPA and the Competition Act, yet their competitive effects remain under-examined in Indian discourse. The RBI's 2018 payment-data localisation mandate, requiring payment system providers to store transaction data exclusively in India, offers the clearest domestic precedent. While framed in terms of regulatory oversight and law-enforcement access, such mandates carry a distinct competitive dimension: compliance requires establishing dedicated in-country server infrastructure, a fixed cost that established, well-capitalised platforms absorb far more easily than smaller fintech entrants or foreign competitors weighing market entry. In this respect, localisation can function similarly to the data-compliance-cost concern this paper raises regarding the DPDPA more broadly — a facially neutral rule that disproportionately entrenches incumbents.

Localisation also interacts with the essential-facility and refusal-to-share concerns discussed earlier in this paper. Where a dominant platform's India-stored dataset becomes practically inaccessible to competitors located abroad, or where localisation requirements are invoked to justify refusing data-sharing arrangements that might otherwise be pro-competitive, the policy risks being deployed as a pretextual shield for exclusionary conduct rather than a genuine data-sovereignty measure. Conversely, localisation can support competition goals where it is paired with mandated local interoperability, preventing a foreign incumbent's global infrastructure advantage from foreclosing domestic entrants who lack comparable cross-border server networks.

The draft Digital Competition Bill and the DPDPA currently treat localisation and cross-border transfer restrictions as data-sovereignty and security matters, without an explicit competition-impact assessment. Given this paper's broader argument for coordinated regulatory design, any future localisation mandate — including the DPDPA's provision enabling the government to restrict transfers to specified countries — would benefit from an accompanying CCI assessment of whether the compliance burden it imposes is proportionate across firms of different scale, rather than being evaluated solely through a data-protection or national-security lens.

BALANCING INNOVATION, REGULATION, AND POLICY RECOMMENDATIONS

Balancing innovation with regulation is a critical challenge in today's digital economy, where rapid technological advancements often outpace existing legal frameworks. Crafting effective policies requires ensuring that regulatory measures protect competition and consumer rights without stifling innovation or discouraging investment in new technologies. Some recommendations are:

1. **Privacy-Enhancing Technologies (PETs):** protect data by limiting exposure or using encryption, anonymization, and differential privacy to safeguard personal information while enabling analysis. These methods align with global data protection frameworks, including India's proposed DPDPA and the EU's GDPR. While PETs help companies comply with privacy laws, reduce legal risk, and attract privacy-conscious consumers, they can also reinforce the dominance of data-rich firms, potentially hindering competition. In India's rapidly evolving digital markets, regulatory oversight is needed to ensure that privacy-driven innovations do not unintentionally produce anti-competitive effects.²⁰

²⁰ Parsheera, Smriti (2022) "India's Policy Responses to Big Tech: And an Eye on the Rise of 'Alt Big Tech'," *Indian Journal of Law and Technology*: Vol. 18: Iss.

1, Article 3
<<https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1113&context=ijlt>> accessed on 12th October 2025



2. **Interoperability and Data Portability to Promote Competition:** Regulators tackling Big Tech dominance must adopt innovative and cooperative strategies, integrating data privacy and competition laws through reforms, collaboration, and new legal approaches. Tools like interoperability and data portability can boost competition by reducing user lock-in. Closer coordination between privacy and competition authorities, as seen in the UK, strengthens enforcement, while integrated legal frameworks address both privacy and anticompetitive concerns.²¹ Courts will shape how privacy violations inform competition law, balancing consumer protection with market freedom. Effective regulation requires expertise, updated laws, and viewing data as both a personal right and a market asset.
3. **Defining Self-Preferencing Under Indian Competition Law:** In India, self-preferencing has been examined in cases like *Umar Javeed v. Google*²² and *Matrimony.com v. Google*²³, but the CCI has yet to define a clear legal test or standard for it. This has sparked debate some view self-preferencing as inherently anti-competitive, while others see it as problematic only when it leads to exclusionary effects. Given the CCI's consistent approach under Section 4 of the Competition Act, it is essential to establish clear thresholds and assess self-preferencing on a case-by-case basis, distinguishing between legitimate competitive conduct and exclusionary practices.
4. **Government interventions:** Governments in India and globally are increasingly acting to address Big Tech dominance. India's Digital Competition Bill, 2024, inspired by the EU's Digital Markets Act (DMA), proposes ex-ante regulations for Systemically Significant Digital

Enterprises (SSDEs), a specialized CCI compliance unit, and faster investigation timelines. The Competition (Amendment) Act, 2023 curbs "killer acquisitions" exceeding ₹2,000 crore and links fines to global revenue. Enforcement actions have targeted Google, Amazon, Flipkart, and Apple for anti-competitive practices. Globally, the EU's DMA imposes obligations on gatekeepers to prevent self-preferencing, ensure interoperability and data portability, and restrict misuse of third-party data. In the US, lawsuits against Meta and Google address anti-competitive acquisitions and monopolistic conduct, while legislative efforts like the American Innovation and Choice Online Act remain stalled.

5. **Integrating Consumer Welfare Beyond Price Metrics:** Traditional competition law measures, focused mainly on prices, are inadequate in digital markets where services are often "free" but paid for with data. Regulators should expand the consumer welfare standard to include privacy, transparency, user autonomy, and choice. Competition assessments should examine how practices such as self-preferencing, data monopolization, and manipulative algorithms affect consumer autonomy and access to alternatives, alongside traditional economic indicators.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: KEY PROVISIONS AND THEIR COMPETITION IMPLICATIONS

Having examined how Big Tech's data advantage translates into market power, and how the CCI has grappled with that reality across cases such as the Google Search Bias matter, the WhatsApp privacy policy case, and *XYZ v. Alphabet Inc.*, it is necessary to return to the statute that opened this paper's inquiry

²¹ Ankit Srivastava and Divyansha Kumar, *Digital Economy, Data, and Dominance: An Indian Perspective*, Journal on Competition Law and Policy, Vol. 2, December 2021, pp. 97-120, <file:///C:/Users/DELL/Downloads/4.+Digital+Econ

omy,+Data,+and+Dominance+An+Indian+Perspective%20(1).pdf> accessed on 12th October 2025.

²² Case No. 39 of 2018

²³ Case Nos. 07 and 30 of 2012



the Digital Personal Data Protection Act, 2023 (DPDPA) and examine its specific provisions in light of the competition concerns this paper has developed. The DPDPA is India's first comprehensive cross-sectoral data protection statute, applying to the processing of digital personal data within India and, extraterritorially, to processing outside India that relates to offering goods or services to individuals in India. Its central obligation is that personal data may be processed only for a "lawful purpose" and only with the data principal's free, specific, informed, unconditional, and unambiguous consent, or under an enumerated "legitimate use."

This consent standard bears directly on the WhatsApp case discussed earlier in this paper. The CCI's 2021 suo motu action against WhatsApp's removal of its opt-out option was, in substance, a competition-law response to a consent design failure — users faced a take-it-or-leave-it choice precisely because WhatsApp's dominance foreclosed any real alternative. The DPDPA now provides a dedicated statutory standard against which such consent practices can independently be tested, meaning future instances of this conduct may attract simultaneous scrutiny under both the Competition Act and the DPDPA. This paper's earlier argument for institutional coordination between the CCI and the Data Protection Board of India is not, therefore, a hypothetical concern but a direct consequence of the DPDPA's own consent framework overlapping with conduct the CCI has already found reviewable.

Second, the DPDPA's proposed "Consent Manager" architecture is directly relevant to this paper's discussion of interoperability and data portability as pro-competitive tools. Structured similarly to the Account Aggregator model this paper examined as an example of open digital infrastructure, Consent Managers could allow users to centrally control and port their consent across competing platforms, reducing the switching costs and lock-in effects that this paper has identified as central to Big Tech's entrenchment for instance, the lock-in dynamics the CCI itself flagged in the WhatsApp matter. Whether

this potential is realised depends on implementing rules ensuring Consent Managers are genuinely interoperable across dominant and non-dominant platforms alike, rather than becoming another feature that only well-resourced incumbents can effectively deploy.

Third, and most directly connected to this paper's central thesis, the DPDPA's uniform compliance obligations data minimisation, purpose limitation, storage limitation, breach notification risk reproducing the very entrenchment dynamic this paper set out to examine in its introduction: that privacy regulation, however well-intentioned, may disproportionately burden smaller competitors while dominant firms absorb compliance costs as a routine cost of business. This is the DPDPA-specific instance of the broader "privacy-enhancing technologies" concern raised in this paper's policy recommendations, and reinforces this paper's argument that data protection and competition regulators must assess compliance costs as a potential barrier-to-entry factor, not merely a consumer-protection matter.

Finally, the DPDPA's "Significant Data Fiduciary" designation — based on the volume and sensitivity of data processed — runs conceptually parallel to the "Systemically Significant Digital Enterprise" threshold this paper discussed under the proposed Digital Competition Bill. Given this paper's recommendation that the CCI and the Data Protection Board coordinate rather than operate in silos, a shared or cross-referenced designation methodology between these two thresholds would be a natural extension of that recommendation, preventing the same large platforms from being independently classified and monitored under duplicative, potentially inconsistent criteria. Read together with the rest of this paper, the DPDPA is thus not a standalone privacy statute but a structural piece of the same regulatory puzzle this paper has argued must be assembled coherently if India is to address data-driven Big Tech dominance effectively.



CONCLUSION AND SUGGESTIONS

The digital economy has redefined the nature of market power, competition, and consumer welfare. Today, personal data has become the cornerstone of competitive advantage, giving companies with vast datasets the power to predict, influence, and shape market outcomes. This has created “data monopolies,” where dominance stems not from price or output but from control over user data and digital ecosystems. As a result, the intersection of competition law and data protection has become vital to ensuring fairness, innovation, and consumer autonomy in the marketplace.

The challenge lies in balancing the benefits of innovation with the risks of data concentration. While Big Data enables personalization and efficiency, it also entrenches incumbents, raises barriers to entry, and limits consumer choice. Global tech giants such as Google, Amazon, and Meta demonstrate how the combination of data control, network effects, and algorithmic power can distort fair competition. Traditional competition law—focused mainly on price-based harm—struggles to regulate “free” services where users pay with their data. Hence, a multidimensional approach integrating competition law, data governance, and privacy protection is essential.

Balancing innovation and regulation demands proportionality. Overregulation may stifle technological growth, while under-regulation enables dominance through self-preferencing, algorithmic bias, and exploitative consent practices. Policymakers must encourage privacy-enhancing technologies (PETs), ensure data portability and interoperability to reduce user lock-in, and clearly define self-preferencing under Indian competition law. Moreover, consumer welfare assessments should expand beyond price to include privacy, transparency, and autonomy.

Effective enforcement requires coordination between the Competition Commission of India (CCI) and data protection authorities to address overlapping

concerns. Strengthening technical expertise, regulatory capacity, and global cooperation is crucial. In conclusion, personal data is now the new driver of market power. A balanced, forward-looking framework that harmonizes privacy, competition, and innovation is essential to ensure fairness and maintain a competitive, inclusive digital economy.

Suggestions

1. **Institutional coordination:** The CCI and the Data Protection Board of India should be brought into a formal coordination framework — whether through a statutory information-sharing gateway or a standing joint forum modelled on the UK's Digital Regulation Cooperation Forum — so that consent design, data concentration, and dominance are assessed coherently rather than in regulatory silos.
2. **Calibrated ex-ante regulation:** The Digital Competition Bill should be finalised with calibrated, evidence-based designation thresholds, a genuine pre-designation hearing, and periodic review mechanisms, ensuring that ex-ante obligations remain proportionate and do not outlast their underlying justification.
3. **Technical capacity building:** The CCI should build dedicated technical capacity — including data-science and algorithmic-audit expertise — to detect algorithmic collusion and assess data-driven theories of harm in merger review, particularly for “killer acquisitions” of nascent, data-rich start-ups.
4. **Strengthening open digital infrastructure:** India should continue to invest in open digital infrastructure such as UPI, the Account Aggregator framework, and ONDC, while actively monitoring these systems for governance capture by incumbents, so that shared infrastructure delivers genuine contestability rather than merely relocating dominance to a new layer.
5. **Expanding the consumer welfare standard:** Regulators should extend the consumer welfare



standard beyond price to encompass privacy, transparency, and user autonomy as measurable competition parameters, and should treat manipulative consent design ("dark patterns") deployed by dominant enterprises as conduct reviewable under Section 4 of the Competition Act.

6. **Proactive monitoring of AI value chains:** As generative AI reshapes the data-compute-distribution triad underlying digital dominance, India should proactively study emerging AI value chains and strategic partnerships between technology incumbents and AI developers, rather than waiting for market structures to entrench as they have in search and social media.

BIBLIOGRAPHY

BOOKS

1. Esayas, Samson Y., *Data Privacy and Competition Law in the Age of Big Data: Unpacking the Interface Through Complexity Science*, Oxford Data Protection & Privacy Law (Oxford, 2024; online edn, Oxford Academic, 18 July 2024)
2. Priyanka Taktwala & Dr. Amrit Subhadars, *Competition Law & Digital Markets in India*, Bharat Law House (16 March 2024)
3. Beata Maihaneimi, *Competition Law and Big Data: Imposing Access to Information in Digital Markets*, Edward Elgar Publishing Ltd (6 February 2020)
4. Alptekin Koksall, *Big Data and Competition Law: Market Power Assessment in the Data-driven Economy*, Routledge; 1st edition (27 June 2025)

ARTICLES

1. Pratyush Prakarsh and Harsh Vardhan, *Competition Law in the Age of Big Tech: Issues and Perspectives*, *International Journal for Multidisciplinary Research*, Vol 6 Issue 6, November – December 2024 <<https://www.ijfmr.com/papers/2024/6/28267.pdf>> accessed on 8th October 2025.

2. Rishita Maheshwari, *The Intersection of Data Privacy and Competition Law: Analyzing Big Tech's Market Dominance*, SSRN Papers, 14th May 2025 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5214841> accessed on 8th October 2025
3. Dr. Mahipal Lather, *Data as a source of market power: Competition law challenges in the age of AI and Big Data*, *International Journal of Law*, Volume 11, Issue 9, 2025, Page No. 19-23, 13-09-2025, <<https://www.lawjournals.org/assets/archives/2025/vol11issue9/11200.pdf>> accessed on 9th October 2025
4. Rupal Nayal, *Data Privacy at the Altar of Competition Laws*, *Journal on Competition Law and Policy*, Vol. 3, December 2022, pp. 79-95 <https://www.cci.gov.in/CCI+-+2022+-+2023_Color-95-111.pdf> accessed on 9th October 2025.
5. Mayank Gandhi, *Big Data and Privacy in Digital Market: A Future Roadmap for Indian Antitrust Authority*, *NLIU Law Review*, Vol XII, Issue I, 2023 <<https://nliulawreview.nliu.ac.in/wp-content/uploads/2023/07/132-154-Vol-XII-Issue-I.pdf>> accessed on 9th October 2025
6. Manu Goswami, *Data Privacy vs. Market Power: Navigating the Intersection of Personal Information Protection and Competition Law in India's Digital Economy*, *Indian Competition Law Review*, Vol. 9, Issue 2, <<http://iclr.in/wp-content/uploads/2024/12/ICLR-Vol-9-Issue-2-Article-4.pdf>> accessed on 9th October 2025.
7. Carolina Abate, Giuseppe Bianco, Francesca Casalini, *The Intersection Between Competition and Data Privacy*, *OECD Roundtables on Competition Policy Papers*, No. 310 <<https://doi.org/10.1787/20758677>> accessed on 10th October 2025.
8. Jay Modrall, *Antitrust risks and Big Data*, *Norton Rose Fulbright* (June 2017) <<https://www.nortonrosefulbright.com/en->



- in/knowledge/publications/64c13505/antitrust-risks-and-big-data> accessed 10th October 2025
9. Kolawole Afuwape, *Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces*, Journal of Digital Technologies and Law, 2024, 2(4) <<https://pure.jgu.edu.in/id/eprint/8973/1/Legal%20Aspects%20of%20Personal%20Data%20and%20the%20Issues%20of%20Competition%20in%20Digital%20Marketplaces.pdf>> accessed on 10th October 2025.
 10. Bruno Lasserre and Andreas Mundt, *Competition law and Big Data: The Enforcers' View* (Bundeskartellamt, 2017) <<https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Fachartikel/Compet>> accessed 10th October 2025.
 11. Daniel Mandrescu, *Tying and bundling by online platforms – Distinguishing between lawful expansion strategies and anti-competitive practices* (2021) 40 Computer Law & Security Review, <<https://www.sciencedirect.com/science/article/pii/S0267364920301047?via%3Dihub>> accessed 02 March 2022.
 12. Shubha Ojha, *Tackling Big Tech's Data Advantage: Is the Indian Regulatory Framework Geared Up?*, Indian Competition Law Review, Volume 6(2), November 2021, pp 55-73, <<http://iclr.in/wp-content/uploads/2024/03/ICLR-Volume-62-Article-5-pp-55-73.pdf>> accessed on 11th October 2025.
 13. Eshita Gupta and Yagya Agarwal, *Big Data Dominance: Underpinning the Separate Relevant Market*, SSC Online Blog, August 23, 2024, <<https://www.sconline.com/blog/post/2024/08/23/big-data-dominance-underpinning-the-separate-relevant-market/>> accessed on 11th October 2025.
 14. Parsheera, Smriti (2022) *"India's Policy Responses to Big Tech: And an Eye on the Rise of 'Alt Big Tech'."* Indian Journal of Law and Technology: Vol. 18: Iss. 1, Article 3 <<https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1113&context=ijlt>> accessed on 12th October 2025
 15. Ankit Srivastava and Divyansha Kumar, *Digital Economy, Data, and Dominance: An Indian Perspective*, Journal on Competition Law and Policy, Vol. 2, December 2021, pp. 97-120, <[file:///C:/Users/DELL/Downloads/4.+Digital+Economy,+Data,+and+Dominance+An+Indian+Perspective%20\(1\).pdf](file:///C:/Users/DELL/Downloads/4.+Digital+Economy,+Data,+and+Dominance+An+Indian+Perspective%20(1).pdf)> accessed on 12th October 2025.