



Data as a source of market power: Competition law challenges in the age of AI and Big Data

Dr. Mahipal Lather

Former Joint Director (Legal), Ministry of Defence, Govt. of India, India

Abstract

In the contemporary economy, data functions as a central strategic input. In markets shaped by digitalisation and artificial intelligence, access to large, diverse, and continuously updated datasets lowers error rates, improves predictive accuracy, and reinforces network effects that can shape competitive dynamics. This paper investigates the ways in which data can generate or entrench market power, the forms in which that power is expressed, and the extent to which competition law and related regulatory frameworks should intervene. Drawing on both economic analysis and recent enforcement activity, it develops a framework for evaluating data advantages across five dimensions, namely scale, scope, speed, substitutability, and sensitivity. The discussion extends to questions of market definition, dominance, and abuse in data-heavy sectors, emphasising the limits of price-focused tests and highlighting the importance of non-price factors such as quality and privacy. Particular attention is given to recent decisions of the Competition Commission of India (CCI), including significant orders against Google, the introduction of a settlements and commitments mechanism in 2024, and the adoption of a “deal value” threshold in merger control aimed at capturing data-driven acquisitions. India’s evolving model is contrasted with the European Union’s Digital Markets Act and the United Kingdom’s Digital Markets, Competition and Consumers Act, with lessons drawn from the UK’s cloud services inquiry into switching frictions such as egress fees. The paper concludes by outlining an enforcement and regulatory toolbox. This includes stricter merger scrutiny for data assets, limited access obligations resembling FRAND terms, measures to strengthen portability and interoperability, constraints on self-preferencing and data combination, support for pro-competitive data intermediaries, and mechanisms to monitor algorithmic collusion. The argument advanced is that competition policy should avoid both extremes: data should neither be assumed to produce automatic monopolisation nor be overlooked as a potential source of exclusion. Instead, a careful and evidence-driven approach is required to safeguard rivalry while maintaining commitments to privacy and security.

Keywords: Data, AI, Market Power, Competition, Interoperability

Introduction

The First Indian Law Commission ^[1] was established in 1834 and was chaired by Lord Thomas Macaulay. Its objective was to examine the power, jurisdiction, and regulations of the courts, police forces, and laws in force in India. The commission made several legislative Data is not oil but a non-rival and replicable resource that depends heavily on context. In digital markets, firms controlling vast and unique datasets gain strong competitive leverage when this data is combined with computing power and model quality, creating feedback loops that improve predictions, recommendations, fraud checks, and monetisation while raising barriers for potential rivals ^[1]. Artificial intelligence deepens existing market dynamics by making training data, fine-tuning corpora, and user interactions central to system performance. High-quality and diverse datasets allow models to improve continually as product use generates fresh feedback. Replicating such data is often difficult, particularly when proprietary or contractually restricted. Even where consumer prices are zero, data confers significant market power. This power does not rest on data alone but grows when combined with computing capacity, model architecture, engineering expertise, and distribution strength. The ability to pool and effectively process data therefore becomes a critical advantage, shaping both competition and innovation ^[2]. Competition law faces three closely connected challenges in data-driven markets. The first is to distinguish when data advantages remain beneficial for innovation and efficiency, and when they cross into exclusionary practices. The second is to adapt

traditional price and output-based tests to markets where concerns of quality, privacy, and developer freedom dominate. The third is to align with privacy and consumer protection regimes, ensuring that enforcement strengthens legitimate data safeguards rather than allowing them to mask anticompetitive conduct. European courts already recognise this overlap, while India’s experience, including major CCI rulings against Google, highlights both opportunities and pressures in regulating data power ^[3]. India has also modernised tools with a settlements and commitments framework and a deal-value threshold in merger control to capture acquisitions of low-turnover but high-value digital targets with “substantial business operations” in India. Alongside competition law, the Digital Personal Data Protection Act 2023 sets the baseline for processing, though it notably omits a portability right present in the GDPR, which affects the feasibility of some pro-competitive remedies ^[4]. Globally, the EU Digital Markets Act (DMA) imposes ex ante duties on designated “gatekeepers,” including restrictions on data combination, self-preferencing, and app store constraints, with further designations in 2024 ^[5]. The UK DMCC Act 2024 gives the CMA targeted powers over firms with strategic market status and is already shaping cloud and mobile ecosystems. The UK cloud investigation underscores how switching frictions like egress fees and licensing rules can entrench incumbents, which maps closely to data portability debates. This paper offers a practical framework to analyse data as a source of market power in AI-intensive markets and to guide case selection, assessment, and remedies under Indian law, while drawing on international experience ^[6].

Literature and Enforcement Landscape: What Makes Data Advantageous?

Academic and policy work since 2015 identifies three channels through which data may contribute to durable power: network effects, learning effects, and switching costs. The OECD's early work on big data and algorithms flagged risks of exclusion and collusion while recognising efficiency gains. Joint analysis by the French Autorité and the Bundeskartellamt framed "data as an asset" that can amplify market power when data is unique, hard to replicate, and linked to scale economies. Subsequent CMA analysis of online platforms found that pervasive default positions, opaque data flows, and restricted mobility of user data supported entrenched positions. A second strand concerns privacy as a dimension of quality. Lower privacy can be an exploitative harm if users have little real choice. The German Facebook case, and the Court of Justice of the European Union's 2023 judgment in *Meta v Bundeskartellamt*^[7], accepted that a competition authority can consider GDPR constraints when assessing abuse, subject to cooperation with privacy regulators. A third strand addresses algorithmic collusion. The OECD has warned that pricing algorithms may make tacit coordination more stable even without an explicit agreement, which challenges traditional cartel tests. Enforcement has adapted. India's 2020 e-commerce market study emphasised platform governance, parity clauses, and search bias. In 2022, the CCI penalised Google in two landmark cases concerning Android restrictions and Play Store billing rules, both of which hinged on default placement, pre-installation, and restrictions on developer choice. The UK and EU have moved toward ex ante constraints that target conduct linked to data control, such as combining personal data across services, self-preferencing in rankings, and limiting downstream access. The UK DMCC regime operationalises bespoke conduct rules and pro-competitive interventions for firms with strategic market status^[8].

A Working Framework: Five "S" Tests for Data Advantage

To avoid treating all data as a barrier, I propose five diagnostic questions for agencies and courts

1. **Scale:** How many observations are needed before model improvement plateaus for the task at issue? Are incumbents in the steep part of the learning curve while rivals are not?
2. **Scope:** Does the holder combine diverse modalities or contexts in ways rivals cannot replicate lawfully or practically? Cross-service combination can amplify prediction in ways that single-service rivals cannot match, which animated both the German and EU concern about data combination. [EUR-Lex](#)
3. **Speed:** How much does freshness matter? In ad tech, fraud detection, or recommendation, stale data can degrade outcomes. If incumbents alone observe at scale in real time, replication costs rise.
4. **Substitutability:** Can rivals buy, license, or synthetically generate functionally equivalent data soon enough to constrain the incumbent? Where contracting or lawful scraping is available at reasonable cost, a barrier claim is weaker.

5. **Sensitivity:** Does the data contain personal or confidential business information such that access remedies would burden privacy or security? If yes, the bar for mandated sharing must be higher, and privacy-by-design sharing or portability is preferable.

The five-S heuristic helps structure evidence on entry barriers and guides the choice of remedies^[9].

Market Definition and Dominance in Data-Rich Settings

1. **Beyond price tests:** Digital services often have a zero monetary price. The relevant competitive dimension is quality, including relevance, latency, security, and privacy. Authorities should employ SSNDQ (small but significant non-transitory decrease in quality) or "attention" and developer-side markets when SSNIP is inapplicable. The CMA's online platforms study and EU policy practice have already shifted toward such quality-based assessments^[10].
2. **Two-sided and multi-sided dynamics:** Data often flows across sides of a platform: user interactions feed ranking, which improves ads or marketplace matching, which finances the free consumer side. Dominance assessment should therefore consider cross-side elasticities and whether rivals can assemble comparable data. This is standard in ad tech, search, marketplaces, and mobile ecosystems^[11].
3. **Dominance indicators with data:** In addition to share and profitability, indicators include control of default positions, ability to degrade privacy without significant churn, unique telemetry, and control of core developer access points (SDKs, APIs, app stores). The CJEU's *Meta* judgment confirms that degradation of lawful processing can be part of an abuse inquiry under conditions^[12].
4. **Theories of Harm: From Exclusion to Exploitation:**
 - **Self-preferencing and foreclosure:** Preferential ranking, default placement, or technical tying that channels data-rich demand to affiliated services can raise rivals' costs. The DMA directly targets such conduct for gatekeepers.
 - **Data exclusivity clauses and MFNs:** Parity and exclusivity rules can prevent business users from multi-homing and starve rivals of data. India's e-commerce study flagged parity clauses and search bias as concerns.
 - **Degrading interoperability or portability:** Technical and contractual friction that blocks switching or multi-homing can entrench incumbents. The UK cloud probe's focus on egress fees and licensing practices is illustrative.
 - **Exploitative data processing:** Where a dominant firm imposes invasive processing terms that users cannot meaningfully avoid, this can reduce consumer welfare even if prices are zero, as seen in the German Facebook matter.
 - **Algorithmic collusion:** Widespread use of pricing and

recommendation algorithms can stabilise tacit coordination. Agencies should watch for “hub-and-spoke” signalling through shared vendors and real-time monitoring that punishes deviation.

India’s Regulatory Innovations in Data-Driven Markets

1. **Landmark abuse cases:** In 2022, the Competition Commission of India (CCI) delivered two landmark rulings against Google, imposing significant penalties that underscored the growing scrutiny of digital platforms in India. The first case examined how Google used contractual terms and technical restrictions in the Android ecosystem to entrench its dominance. By mandating the pre-installation of its own applications and making them the default choice for users, Google limited the ability of device manufacturers and rival app developers to compete on fair terms. The second case dealt with Google’s Play Store billing policies, which compelled app developers to use Google’s proprietary billing system for in-app purchases. This requirement not only restricted developer autonomy but also ensured that data and revenues flowed through Google’s ecosystem, reinforcing its control. Together, these cases highlighted how defaults, pre-installation practices, and restrictive billing rules can distort competition, reduce innovation, and strengthen data-driven market power ^[13].
2. **Settlements, commitments, and penalty guidance:** In March 2024, India operationalised a settlements and commitments regime to resolve abuse and vertical cases faster, accompanied by penalty guidelines and turnover determination rules. This speeds intervention in fast-moving digital markets where delay can tip markets ^[14].
3. **Merger control for data-driven deals:** In September 2024, India brought in a new deal-value threshold to strengthen merger control in fast-growing digital markets. Under this rule, any combination above INR 2,000 crore must be notified to the Competition Commission of India if the target has “substantial business operations” in India, even when its turnover or assets are relatively small. The aim is to capture acquisitions where value lies in users, data, or technology rather than traditional balance sheet measures. Detailed guidance and FAQs explain how the deal-value metric and nexus test will be applied in practice ^[15].
4. **Adjacent regimes:** The Digital Personal Data Protection Act 2023 sets baseline processing rules. It does not provide a GDPR-style portability right, which complicates some competition remedies and shifts focus to safe interoperability and sectoral schemes like Account Aggregators in finance. India’s ONDC illustrates an interoperability approach in e-commerce through open protocols that can lower entry barriers without mandatory sharing of sensitive data ^[16].

Comparative Benchmarks

1. **EU ex ante rules:** The DMA designates gatekeepers and imposes obligations including limits on combining personal data across services without consent, bans on self-preferencing, and requirements around app store

terms. In 2024, Apple’s iPadOS was added to the list of gatekeeper services, with broader enforcement actions launched in early 2024 against several firms ^[17].

2. **UK strategic market status regime:** The DMCC Act 2024 empowers the CMA to set conduct requirements and impose pro-competitive interventions for designated firms, with guidance published in December 2024 and the regime in force in 2025. The CMA’s cloud investigation concluded that competition was not working well and focused on switching frictions including egress fees and licensing. These findings support stronger portability and interoperability in adjacent digital markets ^[18].

Assessing Data Advantages in AI-Intensive Markets

1. **Learning curves and diminishing returns:** Authorities should insist on task-specific evidence that more data meaningfully improves outcomes. In some tasks, returns diminish quickly once diversity thresholds are met. In others, like safety or fraud, rare-event coverage requires significant scale and recency. Parties should provide ablation studies and error-reduction curves. Where substitutes like synthetic data, public datasets, or transfer learning close the gap, claims of insurmountable data moats weaken ^[19].
2. **Data quality, not just volume:** Model performance depends on diversity, label accuracy, and noise filtering. If a rival can replicate functionally equivalent performance with curated or licensed data, the incumbent’s “scale” claim should not by itself prove a barrier.
3. **Lawful access and constraints:** Competition analysis must respect privacy, copyright, and contract. Remedies should avoid forcing disclosure of personal or confidential data unless strictly necessary and safely designed. The DMA’s approach to limiting cross-service data combination without consent provides a template that balances competition and privacy.

Discussion and Suggestions

India’s digital economy has grown rapidly, with platforms, cloud services, and fintech ecosystems creating new forms of market power centred on data. Traditional competition law tools under the Competition Act 2002 must be recalibrated to address acquisitions and conduct where data, algorithms, and network effects play a decisive role. Remedies and policy design must be tailored to the Indian context, where consumer welfare, privacy, and access are all constitutional and regulatory priorities ^[20].

1. **Merger Control:** India was the first to act because, while acquisitions undertaken in the digital sector might never actually be scrutinised, they were bound to be competitively significant. India implemented its deal-value threshold in September 2024. Even though they have low turnover, start-ups and platform firms have massive user bases and data assets. The Competition Commission of India (CCI) should require merging parties to disclose details of the datasets involved, the terms of exclusivity, and the scope for replication by competitors. In designing remedies, structural separation may be inappropriate in rapidly evolving

markets. Behavioural commitments, backed by monitoring, can be more effective. Obligations such as data firewalls and siloing can prevent harmful post-merger data integration. To remain relevant, remedies should include sunset clauses and review mechanisms, recognising that technology standards and privacy norms evolve quickly ^[21].

2. Abuse of Dominance and Vertical Restraints:

Remedies for abuse of dominance and vertical restraints should enhance interoperability, portability, and user choice. India's Account Aggregator framework in finance and the Open Network for Digital Commerce (ONDC) in e-commerce demonstrate how governance and consent dashboards can make data interoperable while respecting privacy. These models show that user empowerment, not forced data sharing, should guide competition remedies. In markets where a platform is unavoidable, FRAND-style access to non-personal and non-confidential data could be considered, but only with strict confidentiality safeguards and independent audits. Default settings and choice architecture also require scrutiny. Self-preferencing in rankings and restrictive anti-steering rules have already been examined in the CCI's Google Android cases. Remedies should ensure fair prompts for browser or search choice and remove contractual barriers that prevent businesses from directly engaging with consumers. In cloud computing, it is essential to cut switching costs. To achieve this outcome limits might have to be placed on egress charges, the legal provisions should contain clear licensing terms that allow competitors to join up and multi-cloud solutions should be welcomed with open arms. The UK's cloud business environment survey would be of great help to India ^[22].

3. Algorithmic Collusion and Market Monitoring:

Where Indian firms increasingly rely on algorithms for pricing; it is likely that the domain of tacit coordination will expand. The CCI should issue regulations on how to manage an algorithmic environment, the need for documenting decisions made by the system and continuous attempts at testing its operation. Sellers of services for price monitoring or algorithmic tools should get some relief ^[23]. The two shouldn't be that far apart and policymakers in India could then look to the OECD or similar rules for guidance these need to be mutated to fit local conditions as, as I pointed out in my earlier post, the marketplaces may at first rotation be filled with many smaller players who are dependent on shared service providers.

4. Coordination with Privacy and Consumer Protection:

The new Data Protection Act 2023 provides a consistent legal framework necessary for the realisation of the DPDB Act 2023. The regulators of different sectors should obtain an explicit memorandum of agreement with the CCI; so, as they are figuring out their own turf, the Reserve Bank of India and, indeed, also the Data Protection Board (tasked not to have conflicting mandates) could collaborate with each other coordination could integrate consumer claims, privacy protections and antitrust remedies ^[24]. The Janus face of

privacy and competition in online markets is nowhere clearer than in the European Court of Justice's ruling in the case *Meta v Bundeskartellamt*. The observations of Chief Justice Mahajan in the aforesaid case will hold well with full force in our case too.

Way Ahead for India

Regulating digital markets in India: Policy learning not one-size-fits-all approaches to case prioritisation and evidence-based analysis Unfamiliar remedies and whether it is a good fit with data protection regimes are just two such concerns. The CCI would need to divert its enforcement work on those cases where the bottleneck and default venues through which the incumbent firms control the markets would not be easily replicated by the challengers. These bottlenecks could be code heading libraries (API), software development kits (SDK), app stores, and calibrated data which provide some platforms with scale benefits ^[25]. You have to start getting a handle on those big players in the system and think about some guiding principles. An eloquent playbook of evidence is also important to enforcement. Instead of relying on the types of rigid categorizations established for typical market studies that the CCI was quick (and dramatic) to reject, the CCI could embrace methods like ablation studies, switching-cost analyses or developer survey methods. Although they are fashions, they have the power to design decision, they can influence the intersection of information and contact clause in legal document and they do shape the opponent behaviour and the consumer conduct. Horns up evidence would allow tough pools to appear clear (there's hardly much of a point any more too really hard work), just as arguments yield subtler signs. With respect to remedies, the new settlements and commitments regime in India is a very inherently flexible instrument. At least the CCI can lap it up on short-term measures which are of course to the benefit of competition and therefore supported by clear monitoring methods. It's a particularly sensible approach when looking at fast-emerging circular economy regions and electric vehicle systems where a delay may reset competitive landscapes for the long-term. Another significant issue under the conditions of the complete implementation of the national market regulation is the compliance with the 2023 Digital Personal Data Protection Act. If there is no explicit grant of portability rights, it is very clear that interoperability remedies must require user consent and privacy-preserving architectures rather than open-ended data sharing. This would ensure the protection of user rights on one side, and a level playing field on the other. Finally, we recommend that an entry barrier be cut in India with investment in public infrastructure. Sectorial data intermediaries and standard organizations are building governance for an open interoperable ecosystem which protects privacy and innovation: The financial sector has Account Aggregator system; e-commerce has its cartridge ONDCs (Open Network for Digital Commerce); adhoc cooperation among central banks is visible with global initiatives too ^[26].

Conclusion

But when it is always new and just requires a few technical control points like an API to get leverage out of that, then data is not just the new vertical industry backbone, but it's something qualitatively different than anything that we have ever known before. But there's a second reason this force

will at least be held up in its current shape. AI reinforces that kind of work in the industry of feedback loop, but its weapon is consolidation. Once this mode of production has taken on a thing-like character like this, it has its own mechanisms of enclosing back on itself and solidifying that structure. Once the laggard can't catch up, it's a long way down. Also, just because you do have the data that people want, that doesn't mean you have a shield from competitors at all. The biggest question is whether that new kind of information is replicable, if rivals can piggyback onto it on the cheap, and how high switching costs pose barriers to competition. Because in the first place competition law must be rooted in empirical knowledge not blind faith. These problems should be enforced based on the learning curve, substitutability, and user switching behaviour. Solutions should be carefully designed to increase user and business choice and at the same time to ensure that privacy and Security are not violated. India has already taken important steps, with deal-value thresholds and a new settlements and commitments framework that enable more expeditious decision of cases. And a few of mean ways to play fast-moving digital markets. After all, ex ante (advance mandatory) obligations, interoperability solutions for identified problems, and lower switching costs in remedies are all fundamental lessons of the EU and UK experience. In addressing this concern, India should use vigilant merger review in conjunction with codes of conduct to deter exclusionary use of data as well as anywhere and safe portability, wherever this is practicable. A reasonable approach can help protect lively competition, keep the door open for entrants and force the former State-owned companies to work for their money, and then some, with someone else's data.

References

- Vashishth TK, Sharma V, Kumar B, Sharma KK. Cloud-Based Data Management for Behavior Analytics in Business and Finance Sectors. In *Data-Driven Modelling and Predictive Analytics in Business and Finance* Auerbach Publications, 2024, 133-155.
- Kumar A. Language intelligence: Expanding frontiers in natural language processing. John Wiley & Sons, 2024.
- Sankhala S, Sinha A. Google v CCI: A Tussle over the Monopoly Culture in the Android Ecosystem. *Jus Corpus LJ*,2024;5:607.
- De Corniere A, Taylor G. Data and competition: A simple framework. Toulouse School of Economics.
- Cabral L, Haucap J, Parker G, Petropoulos G, Valletti TM, Van Alstyne MW. *et al.* The EU digital markets act: a report from a panel of economic experts. Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., and Van Alstyne, M., The EU Digital Markets Act, Publications Office of the European Union, Luxembourg, 2021.
- Whelan P. Software Licensing and the UK's Cloud Services Market Investigation: A Missed Opportunity to Remedy Anticompetitive Practices?. Available at SSRN 5332643, 2025.
- Meta Platforms Inc. and Others v Bundeskartellamt, Case C-252/21, ECLI:EU:C:2023:537 (CJEU, 4 July 2023).
- Ghosh N, Malik R. The Structural Role of Private Enforcement in Digital Markets: An Indian Competition Law Perspective. *NLIU L. Rev.*,2023;13:126.
- Day GS, Wensley R. Assessing advantage: a framework for diagnosing competitive superiority. *Journal of marketing*,1988;52(2):1-20.
- Reyna A. The psychology of privacy—what can behavioural economics contribute to competition in digital markets?. *International Data Privacy Law*,2018;8(3):240-252.
- Pontual Ribeiro E, Golovanova S. A unified presentation of competition analysis in two-sided markets. *Journal of Economic Surveys*,2020;34(3):548-571.
- D'Amico A, Pelekis D, Santos CT, Duivenvoorde B. Meta's Pay-Or-Okay Model: an analysis under EU data protection, consumer and competition law. *Technology and Regulation*, 2024, 254-272.
- Dalvi M, Gadkari A. CCI and regulation of digital platforms and blockchain: Will it take a rule of reason; per se or a schizophrenic approach?, 2022.
- Sangwan AS, Sharma BL, Kumar Y. *Recent Development in India@ 2024*.
- Choudhary MP. *MERGER & ACQUISITIONS: A COMPETITION LAW PERSPECTIVE*. Chyren Publication, 2024.
- Alkhamsi NN, Alqahtani SS. Compliance Framework for Personal Data Protection Law Standards. *International Journal of Advanced Computer Science & Applications*,2024;15(7).
- Ingemarsson R, Bichet P. Survey on the digital markets act and digital policy: a year into the application of one of the most innovative regulatory tools (2023–2024). *Journal of European Competition Law & Practice*,2024;15(5):330-338.
- Mantri A, Kaltenbrunner L, Frankel A, Bennett O, Jagoe S. Cloud services: market reflection and a growth story. *Competition Law Journal*, 23(1), 42-49.
- Zhou X, Sun Y, Wu J, Huang X. How to systematically develop an effective AI-based bias correction model?. *arXiv preprint arXiv:2504.15322*, 2025.
- Esayas SY. Data privacy and competition law in the age of big data: Unpacking the interface through complexity science. Oxford University Press, 2024.
- Kapadia H. Dissecting the Competition Commission of India's Regulatory Framework for Combination Approval. *Issue Indian JL & Legal Rsch.*,2023;5(2):1.
- Contreras JL. A brief history of FRAND: analyzing current debates in standard setting and antitrust through a historical lens. *Antitrust Law Journal*,2015;80(1):39-120.
- Baron JR, Armstrong KE. The Algorithm in the C-Suite: Applying Lessons Learned and Information Governance Best Practices to Achieve Greater Post-GDPR Algorithmic Accountability. In *The GDPR Challenge*. CRC Press, 2021, 14-35.
- Aggarwal U, Singh J. Sectoral Regulators v CCI: Jurisdictional Challenges under the Competition Act 2002. *Jus Corpus LJ*,2024;5:152.
- Zilahi R. Mobile App & Backend Integration for Streamlined Library Operations: Approach with Cutting-Edge Technology, 2023.
- George AS, George AH. Open network for digital commerce (ONDC): Democratizing digital commerce and curbing digital monopolies in India. *Partners Universal International Research Journal*,2022;1(2):92-102.