Enhancing Regulatory Coordination: Balancing Competition and Data Protection in Digital Markets

DGN Research Paper 6

Neha Jain
Sharmadha Srinivasan

March 2024

Working Paper 6
March 25, 2024

About Data Governance Network

The Data Governance Network is a self-sustaining, multidisciplinary community of experts which brings institutions, individual experts, and stakeholders from industry, government, and academia together through its data-backed research, policy discussions, and convening activities. This results in insightful and varied knowledge exchange contributing to the enhancement of technology-focused policy research.

About Artha Global

Artha Global is a policy organisation that supports global partners to design, implement, and institutionalise practices that promote prosperity and resilience, with a primary focus on the developing world. We provide actionable research, support policy implementation and work to institutionalise change. We believe that the multiple challenges of the 21st century require new thinking that cuts across the traditional boundaries of geography, disciplines and interests. Therefore, we leverage our global network of experts to help craft new development agendas, create consensus and build broad coalitions across governments, business, academia, philanthropy and civil society. Artha's research is housed in six centres: **Emerging Cities, Access to Justice, Technology and Innovation, Rapid Insights, Public Health, and Inclusive Growth.**

Disclaimer & Terms of Use

Suggested Citation

Jain, N., & Srinivasan, S. (2024). "Enhancing Regulatory Coordination: Balancing Competition and Data Protection in Digital Markets." Working Paper. Mumbai: Artha Global

Acknowledgements

We would like to thank Dr. Niranjan Rajadhyaksha, Dr. Hemant Adarkar, Vikram Sinha, and Sridhar Ganapathy for their invaluable contributions and support throughout the research process. Additionally, we would like to thank Naisha Khanna and Aastha Doshi for their editorial inputs. All the contributions have been instrumental in shaping this work.

Abstract

With the enactment of the Digital Personal Data Protection Act (DPDP) and the subsequent establishment of the Data Protection Board, potential clashes between competition and data issues may arise between the Board and the Competition Commission of India (CCI). This regulatory overlap may extend beyond jurisdictional matters and could lead to unique conflicts, where the pursuit of data protection might conflict with promoting competition in data-driven market. The paper offers an overview of past regulatory battles in India and the mechanisms employed to resolve turf battles. Given the absence of coherent mechanisms in the past, it emphasises the need for an effective framework focused on coordination and cooperation between regulators to address conflicts. By outlining this framework, the paper underscores the importance of striking a balance between competition and data protection considerations to achieve an optimal outcome that fosters competitive markets while safeguarding user privacy.

Table of Contents

Introduction

The recently filed civil antitrust lawsuit against Apple Inc. has drawn attention to the well-known challenges posed by data-driven digital platforms.[1] In 2023, the Department of Justice (DOJ) filed two similar antitrust cases against Google, alleging that Google's prioritisation of its own services in search results and its utilisation of user data to dominate the ad tech space had given it an unfair competitive advantage in the digital market.[2] Allegations against these tech giants underscore the pivotal role of data in digital markets. The role of data is complex and rapidly evolving, with profound implications for businesses and consumers alike.

Traditionally, consumer welfare in competition literature was measured through the lens of price. However, there has been a notable conceptual shift in evaluating consumer welfare in data-driven markets. Increasingly, it is assessed on the utilisation, collection, and accessibility of data (Cho, 2023). This transition is driven by the recognition that data significantly influences competition dynamics in the market.

Vague, complex, and lengthy consent clauses for data collection create information asymmetry that favours the data collector—primarily dominant digital platforms. Second, consumer data allows businesses to understand consumers' tastes and preferences, which enables platforms to optimise the user experience (Vanberg and Unver, 2017). This contributes to network effects that increase barriers to entry based on data, which adversely impacts competition in the market. Third, zero-price strategies employed by data-driven businesses create biases in consumer behaviour, once again providing an unfair advantage to businesses with large databases. Utilising data in this way poses anti-competitive challenges and also creates privacy harms to citizens in the long term. These concerns have prompted legislators and regulators to scrutinise data-fueled business models and the market behaviour of digital platforms.

The 2019 *Bundeskartellamt landmark* Facebook[3] ruling offers a glimpse of what modified antitrust regulation considering data-related concerns might entail. An updated legal toolkit, however, would not only necessitate antitrust law taking into consideration data protection-related concerns, such as lack of user control over personal data, but also actively seek to redesign the regulatory framework for effective implementation.

Competition regulators will need to work closely with regulators overseeing data protection. It would demand the establishment of a normative framework that acknowledges these overlaps and draws upon data protection principles where applicable (Kira, Sinha, and Srinivasan, 2021). This approach draws from established practices in other regulatory domains; for example, banking and finance fall under the jurisdiction of multiple regulators, ranging from central banks to securities and insurance watchdogs.

[1] For more details on the DOJ case against Apple, read the department's press release

[2] For more details, read the New York Times article

[3] Bundeskartellamt prohibits Facebook from combining user data from different sources. See the report here.

India is behind the curve in both a recalibrated regulatory approach and implementing it. Establishing such an approach is particularly crucial in India due to historical issues, in which unclear jurisdictions and the absence of a framework for regulators to consult on overlapping matters have sparked turf battles. These conflicts, such as the one between the Reserve Bank of India (RBI), a sectoral regulator, and the Competition Commission of India (CCI), a cross-sectoral regulator, over the control of banking mergers, have resulted in significant uncertainty and delays, with costs to the regulators, the regulated entities, and the market.[4]

While the CCI has now acknowledged that privacy and data protection considerations must be integrated into the competition policy framework,[5] there is currently no roadmap to guide this process. Even the proposed Competition (Amendment) Act 2023, does not address data considerations.

With the passage of the Digital Personal Data Protection Act, significant impacts on digital business models and competition dynamics are expected. Data-related competition issues will also likely pose greater challenges in terms of regulatory coordination. Unlike previous clashes between cross-sectoral and sectoral regulators, both regulators in this instance—the CCI and the Data Protection Board established by the Digital Personal Data Protection Act—are cross-sectoral. Thus, adopting a synergistic approach to digital antitrust is crucial.

Building on our work on a normative framework for competition regulation and data protection overlaps in India (Sinha and Srinivasan, 2021), this paper will propose broad-level recommendations for preventing and addressing regulatory conflicts between the CCI and the Data Protection Board, with an aim to extract principles to foster competitive digital markets.

The paper is structured in the following manner: Section II provides an overview of the predominant reasons for regulatory conflicts, extrapolating from past examples in India and the subsequent costs of conflicts on businesses and the market. Section III highlights the effects of the DPDP Act and other dynamic issues in the market on individual data protection rights and competition. Section IV classifies the multiple scenarios that could arise in the realm of data protection and competition and recommends changes. Section V outlines broad-level recommendations that could decrease the likelihood of regulatory conflicts and help establish competitive markets.

[4] For more information on the tussle between the CCI and RBI over the control of mergers, read this article in the Business Standard.

[5] CCI study: Data privacy can take form of non-price competition

Causes and Costs of Regulatory Turf Battles in India

This section examines the reasons for turf battles among various regulators and the resulting cost externalities imposed on businesses and the market. A review of case histories in India indicates several factors contributing to these conflicts, primarily arising from overlapping jurisdictions, varied interpretations of legislative mandates, and jurisdictional ambiguities in legal interpretations. Below, we outline the primary reasons for regulatory conflicts supported by case histories:

1. **Ambiguous legislative language leading to a broad overlap of jurisdiction**: Ambiguous legislative language within each regulator's distinct legislation leads to overlapping jurisdiction and blurred distinctions between regulators. This ambiguity creates challenges for regulators when implementing measures to address disputes that arise among market participants. Unclear directives regarding the role of each regulator significantly contribute to regulatory disputes in India. Below are two prominent examples from the past:

A. CCI and Petroleum and Natural Gas Regulatory Board (PNGRB) [2011]

The PNGRB was established under the Petroleum and Natural Gas Regulatory Board Act in 2006,[6] with the primary objective of regulating the petroleum and natural gas sector in India. Its mandate involves safeguarding consumer interests by promoting fair trade and fostering healthy competition among entities operating in the sector. This mandate is similar to the CCI's general mandate to regulate competition across all sectors in the country.

In 2011, Reliance filed a complaint with the CCI alleging that its rivals—Indian Oil Corporation, Bharat Petroleum, and Hindustan Petroleum—formed a cartel for the supply of aviation fuel for Air India. During the investigation, the three companies challenged the CCI's jurisdiction in the conflict. Subsequently, they filed a complaint with the Delhi High Court, claiming that the matter fell under the jurisdiction of the PNGRB. Broad overlapping jurisdiction between the two regulators created uncertainty over which regulator was best placed to address the alleged anti-competitive behaviour of the market participants. The High Court issued an interim order stating that the CCI did not have jurisdiction over the matter, despite the fact that the PNGRB Act did not grant the sector regulator exclusive jurisdiction.

This decision undermined the authority of the CCI and created uncertainty about its role in regulating the Petroleum and Natural Gas sector. It also created uncertainty for market participants, impacting investments and hindering the smooth functioning of the industry.[7]

B. CCI and Telecom Regulatory Authority of India (TRAI) [2017]

The TRAI was established under the Telecom Regulatory Authority of India Act in 1997 to promote competition and ensure the growth of the telecom sector in India.[8] TRAI is also tasked

[6] The Petroleum and Natural Gas Act Regulatory Board Act, 2006
[7] For more details on the impacts of regulatory overlaps in India, read this paper.
[8] The Telecom Regulatory Authority of India Act, 1997

with creating an environment to facilitate fair competition in the market—a legislative mandate that broadly overlaps with that of the CCI.

In 2017, Reliance Jio filed a complaint with the CCI, alleging cartelization by Airtel, Vodafone, and Idea—the dominant telecom operators in the industry. The incumbents challenged the CCI's jurisdiction to investigate the matter, arguing that the TRAI, as the sector-specific regulator, was the appropriate authority to address issues related to telecommunications services. This matter was escalated to the Supreme Court of India, which ruled that the TRAI held the power to first determine the rights and obligations of the parties. Then, if the TRAI believed that anti-competitive activity had occurred, the CCI's jurisdiction would be invoked.

The prolonged legal battles and resulting uncertainty impacted the regulatory landscape in the country and also led to an uncertain business environment in the telecom industry.[9]

2. **Common legislative language leading to an overlap of jurisdiction**: The second reason for regulatory conflict arises from a more specific legislative overlap rather than a broad overall mandate. It occurs when the sectoral regulator is granted legislative authority to check and address "anti-competitive behaviour" in the market—employing legislative language *identical* to that found in the Competition Act and mimicking the role of the CCI.[10] We have outlined three prominent examples of this type of conflict.

A. CCI and Delhi Electricity Regulatory Commission [2017]

The Electricity Act of 2003[11] empowers the Delhi Electricity Regulatory Commission (DERC) to issue directions to a licensee if it enters into any agreement or abuses its dominant position, causing an adverse impact on competition in the electricity sector. These legislative powers are nearly identical to those of the CCI.

In 2017, the CCI issued notices against BSES Rajdhani Power, Yamuna Power, and North Delhi Power, accusing them of abusing their dominant positions by engaging in unfair and discriminatory practices. The DERC questioned the CCI's intervention, asserting that addressing anti-competitive behaviour by market players in the electricity sector fell under its jurisdiction as per the Electricity Act. Having two regulators with identical legislative responsibilities blurs the distinct roles these regulators are intended to play, increasing the risk of regulatory conflicts.

This matter escalated to the judiciary, which ruled that specific technical and sector-focused issues related to electricity should first be addressed by the DERC, and then by the CCI. This ruling undermined the authority of the CCI and the prolonged legal battle created uncertainty for market participants.[12]

---

[9] To learn more about the link between regulatory uncertainty and market behaviour in the telecom industry, read this paper.
[10] To learn more about specific legislative overlap in India, read this paper.
[11] The Electricity Act, 2003
[12] To learn more about the impact of regulatory conflicts on the functioning of the market read this article.

B. CCI and Securities and Exchange Board of India (SEBI) [2021]

SEBI was established under the SEBI Act of 1992.[13] Through this Act, SEBI's regulatory framework is designed to prevent unfair trade practices. SEBI also assumes a supervisory role in "[inspecting], [investigating], and [initiating] proceedings against credit rating agencies." These legislative responsibilities overlap with those of the CCI.

In 2021, the National Highway Authority called for tenders of different credit rating agencies—CRISIL, India Ratings and Research, CARE Ratings, and ICRA—to rate their bonds. After the agencies submitted bids that were similarly priced, an informant filed a complaint with the CCI. SEBI, however, objected to the CCI's jurisdiction, claiming that the matter fell under its regulatory purview. Despite SEBI's objections, the CCI proceeded, citing its mandate to investigate anti-competitive practices across all sectors, including those regulated by other statutory bodies. Having two regulators—the CCI and SEBI—with nearly identical legislative language created uncertainty in their distinct roles and resulted in this conflict. This conflict affected the regulatory landscape and the market participants.[14]

C. CCI and RBI [2013]

The RBI was established under the Reserve Bank of India Act of 1934.[15] In addition to controlling the country's monetary policy, the RBI is responsible for regulating the banking sector in India and also controls mergers and acquisitions of banks and their subsidiaries. The RBI has contended that the banking sector must be excluded from the ambit of the competition commission, especially in matters of mergers and acquisitions, believing it has the required expertise and competence to deal with such matters. This request was declined, leading to situations where both the RBI and CCI had concurrent jurisdiction over bank mergers and acquisitions. Ultimately, however, in 2017, the government carved out an exception for Regional Rural Banks (RRB) that were set up under the RRB Act of 1976.[16] For a period of five years, these banks would not need approval from the CCI to merge. With a banking sector that was strained, the decision was made in the matter of public interest to decrease the number of regulatory approvals.

3. **Differing regulatory approaches between the CCI (horizontal regulator) and sectoral regulators**: Competition law plays a crucial role in safeguarding competition in the market and is an integral component in establishing a free market economy. In the context of India's market-driven economy, sectoral regulators have been instituted to address technical, sector-specific issues. These regulators have an 'ex-ante regulatory' approach, which means they anticipate and intervene in potential issues before they arise. Through this approach, sectoral regulators mandate market players to act in a certain way and focus on "attenuating the effects of market power" by facilitating the organised development of their respective sectors. In contrast, the CCI, employs an 'ex-post regulatory' approach and addresses issues

[13] Securities and Exchange Board of India Act, 1992
[14] To read more about the impact of regulatory conflicts on policy and administrative timeline, read this article.
[15] The Reserve Bank of India Act, 1934
[16] The Regional Rural Banks Act, 1976

that arise if actions taken by market participants impact competition. Through this approach, the CCI focuses on correcting the abuse of dominant power by market players.

While sectoral regulators and the CCI both aim to enhance economic performance and prevent market power concentration, they differ in their legislative mandates. The divergent ex-ante and ex-post regulatory approaches may lead to conflicting decisions and interpretations of competition-related issues. This can decrease the effectiveness of competition policy, adversely impacting the development of a predictable regulatory environment and making it challenging for market participants to anticipate and align with regulatory expectations. This, in turn, may impede fair competition, affect market dynamics and regulatory credibility, and undermine the overall goal of fostering a competitive market.[17]

[17] For more information on how divergent approaches by cross sectoral and sectoral regulators impact the market, read this paper.

Table 1: Mapping of regulatory conflicts in India

Regulators Involved	Year	Type of regulators	Reason for Regulatory Conflict	Summary of Issue
CCI and PNGRB	2011	Cross-sectoral regulator and sectoral regulator	Broad legislative overlap	CCI's jurisdiction to look at anti-competitive practices in the petroleum sector was challenged.
CCI and TRAI	2017	Cross-sectoral regulator and sectoral regulator	Broad legislative overlap	CCI and TRAI both laid claim jurisdiction over anti-competitive issues in the telecom industry.
CCI and DERC	2017	Cross-sectoral regulator and sectoral regulator	Specific legislative overlap	The DERC claimed jurisdiction over anti-competitive practices in the electricity sector.
CCI and SEBI	2021	Cross-sectoral regulator and sectoral regulator	Specific legislative overlap	Jurisdictional conflict between SEBI and CCI on regulating credit rating agencies.
CCI and RBI	2013	Cross-sectoral regulator and sectoral regulator	Specific legislative overlap	The RBI wanted banking mergers to be outside the domain of the CCI.

Source: Authors' analysis based on secondary research

Regulatory overlap complicates policy objectives and hampers the formulation of clear and effective regulations.[18] When the roles of regulators are unclear due to this overlap, conflicts can arise, especially when regulators establish rules with inconsistent standards. Such conflicts impose tangible costs on businesses and breed uncertainty for both businesses and investors, impeding the smooth operation of regulatory frameworks (Robb et al., 2023). In India, resolving regulatory conflicts often face delays, leading to inefficiencies in addressing issues crucial for upholding market integrity and promoting fair competition, consequently undermining the effectiveness of regulators.

[18] See the Regulatory overlap: A systematic quantitative literature review paper for more details.

Classification of conflicts: A Contestable Market Analysis

Conflicts between cross-sectoral and sectoral regulators, as outlined above, impose tangible costs on businesses and consumers and impede the smooth functioning of the market. Data-related competition issues are expected to pose even greater challenges in terms of regulatory coordination, as both the CCI and Data Protection Board are cross-sectoral regulators.

This section will classify the multiple scenarios of conflict that could arise in the realm of data protection and competition stemming from provisions in the Digital Data Protection Act and potential market-related issues. The analysis will be based on the contestable market theory,[19] with the search engine market serving as the context.

A. Data protection and competitive outcomes stemming from how current laws stand

1. Mandatory consent on data collection

Section 6, sub-section 1, of the DPDP Act, requires Data Fiduciaries to obtain "free, specific, informed, unconditional, and unambiguous consent" from Data Principals before collecting, processing, or sharing their personal data.

Through this provision, obtaining consent serves as the legitimising factor for any data-related practices, promoting transparency and granting greater autonomy to data principals during data processing (Mills, 2022). This provision could, however, give incumbent firms a significant advantage over newer competitors. Potential entrants in the market may face barriers to entry due to the additional 'barrier' of obtaining consent and building databases, a challenge that incumbents with existing databases may not encounter.[20]

2. Exception to mandatory consent on data collection

Section 7, sub-section b, of the DPDP Act, lays out exceptions to seeking consent for data collection. While in most instances, data fiduciaries need consent before engaging in data practices, government agencies, their instrumentalities, and businesses that process data for the purpose of "national security" are exempt from this law and are not required to seek consent from consumers.

Introducing an exception to the mandatory consent law has detrimental effects on data protection for consumers. It creates opportunities for entities handling data to exploit it, by retaining and processing it for purposes beyond those specified. This violates the right to privacy, which could lead data principals to lose control over their data, as power imbalances are created between data fiduciaries and principals. This provision's exception also carries negative implications for competition. Public sector actors may gain an advantage over private

[19] The contestable market theory argues that companies with a few rivals in a market with weak barriers to entry behave competitively because of the fear of being driven out of the market.

[20] For more details and examples on when data creates a competitive advantage, please see this article.

sector entities due to greater exemptions for data processing accorded to them, thereby increasing the possibility of aggregating databases. Anirudh Burman (2023) suggests that this exception "significantly empowers the state and places state imperatives on a different pedestal compared to private entities." By making it more challenging for private firms to compete with public actors, the exception creates opportunities for public sector firms to behave anti-competitively.

3. Requirement of notice for collection and processing of data

Section 5, sub-section 1, of the DPDP Act, also stipulates that data fiduciaries must furnish a notice to data principals prior to soliciting consent for the processing of personal data. This notice is mandated to contain specific details regarding the personal data to be collected and the intended purpose of its processing.

Such detailed information serves to benefit consumers in terms of data protection, as it restricts opportunities for the exploitation of their data while enhancing transparency in the processing procedure. This transparency, in turn, nurtures trust between data principals and fiduciaries, as data fiduciaries are held to a high standard for handling and utilising personal data. While this provision enhances consumer privacy, it introduces compliance obligations and costs to new businesses. These costs could include legal consultation to ensure the notice complies with the law and administrative costs associated with maintaining up-to-date notices and managing data subject requests.[21]

4. Exception to requirement of notice for collection and processing of data

Section 17, sub-section 1 of the DPDP Act empowers the central government to exempt certain data fiduciaries or classes of data fiduciaries, including some startups, of certain obligations regarding the provision of a notice for the purpose of data collection.

This exception in the provision could decrease transparency and create power imbalances between data principals and fiduciaries. Reducing accountability mechanisms for entities handling personal data can increase opportunities for them to exploit data, negatively impacting data protection possibilities. Moreover, this provision's exception also has negative implications for competition. Public-sector firms may have a competitive advantage over private-sector firms, which are likely to face greater regulatory hurdles.

5. Reporting of personal data breach by all firms

Section 8, sub-section 6, of the DPDP Act mandates prompt reporting of every personal data breach to the Data Protection Board of India by data fiduciaries, including information on affected data principals.

This provision yields positive outcomes for data protection, as it ensures data principals are informed of any violations, thereby increasing transparency and granting data principals

[21] To read more about the impact of strict data regulations on firms, please read this.

greater control over their data. This clause, however, carries negative implications for market competition. Detecting data breaches promptly may require technological investments, such as implementing privacy-by-design principles, which smaller firms might find difficult to afford. Additionally, for second-hand data processing, firms may prefer larger entities with stronger breach protection capabilities, potentially leading to data concentration among a few major players. While data accumulation[22] is not inherently a barrier to entry, the likelihood of concentration may challenge fair competition (Nuccio, 2017).

6. Grievance redressal by a Data Fiduciary

Section 13, sub-section 1, of the DPDP Act, establishes that data principals have the right to seek grievance redressal if the entities handling their data fail to comply with data protection standards.

This provision aims to empower data principals by providing them with effective means to address concerns related to their data. The imposition of penalties for non-compliance creates accountability, encouraging data fiduciaries and consent managers to implement and adhere to robust standards for the protection of personal data. However, larger firms, with greater technical and financial resources, may find it relatively easier to comply with the regulatory requirements in comparison to smaller firms (Johnson, et al., 2020). This could, in turn, raise barriers to entry and decrease competition in the market.

B. Data protection and competitive outcomes stemming from dynamic issues in the market

1. Data Portability provision for firms

The implementation of data portability would reduce the burden on data transfers, enabling consumers to switch easily between providers while taking their data with them (Vanberg and Unver, 2017). Although the absence of this provision has minimal implications for data protection, its absence significantly affects market competition. A data portability clause would likely grant individuals greater control over their data, thereby positively impacting data protection by empowering individuals with control over their data. Conversely, the lack of this provision could negatively impact market competition. High switching costs between service providers could lead to consumer lock-in, discouraging users from switching services due to the fear of data loss. Such consumer lock-in could render the marketplace more susceptible to exclusionary practices by dominant players (Vanberg and Unver, 2017). Additionally, when firms have consumer security due to high switching costs, barriers to entry rise, harming competition in the market. Rubinfeld and Gal (2017) suggest that technological, legal, and behavioural barriers may arise not only during data collection but also during storage and usage (analysis) of information. Therefore, regulators should prioritise ensuring consumers' ability to switch products or platforms freely, anywhere and anytime, over merely accumulating large quantities of data. Introducing a data portability provision would

[22] For more details on the impact of data accumulation on competition, please see Propensity of Data Accumulation to Raise 'Barriers to Entry'

strengthen the Act by reducing switching costs and mitigating network effects that threaten competition in the marketplace (Vanberg and Unver, 2017).

2. Mergers and acquisitions in data-driven markets

The DPDP Act does not explicitly prohibit mergers between companies with similar data-driven businesses. The merger between WhatsApp and Facebook serves as an illustration, where WhatsApp indicated its intention to share consumer data with Facebook. The absence of such a provision undermines individuals' data protection rights in the market. Allowing mergers between similar data-driven businesses enables firms to consolidate market power by accumulating more consumer data. This concentration hampers the ability of more efficient entrants to displace incumbents, as new players struggle to amass a sufficient critical mass to enter the market (Srinivasan et al., 2023). Additionally, businesses that leverage past data and historical patterns, inaccessible to new competitors, enjoy a competitive advantage and can better serve their customers. This further raises barriers to entry and impedes competition in the market.[23]

3. A big tech platform manipulating search results to benefit platform players

In the market, existing players tweaking results to benefit their own subsidiary businesses limit consumer choice, allowing businesses to undermine competition and data protection rights. For instance, Google made algorithmic changes to its search results to prioritise its own products and services, often at the expense of competitors and external websites. This strategic decision by Google to leverage its dominance as a search engine doubled its revenues nearly five times and significantly decreased competition in the market. A study found that a user would have to scroll 42 percent down the page before reaching the first “organic” search result.[24] Additionally, Apple has made it considerably harder for third-party apps to collect data by introducing an enhanced notice and consent mechanism based on user opt-in while exempting its own apps from this provision.[25] Allowing bigger businesses to establish their own standards of compliance with respect to data collection raises barriers to entry and has the potential to drive smaller firms out of the market.

[23] For more detail on the relationship between data and competitive advantage, please read this article.
[24] For more detail on the impact of Google’s practices on competition, please read this article.
[25] For more detail on Apple’s privacy features, please read this article.

Conflict Severity: Assessing Impact on Data Security and Competition Objectives

Drawing from the examples discussed in the previous section, this section will classify the level of conflict severity, assigning a number from 1 to 5. The classification depends on two factors: the impact of legislative provisions or market participant behaviour on data security and competition objectives, and the necessary actions to resolve these conflicts.

A '**Level 1**' classification is assigned when a provision in either law positively impacts both competition and data protection. For instance, under the DPDP Act, data fiduciaries are only allowed to process data for lawful purposes. This provision enhances data protection by giving users greater autonomy over the data they share, as it decreases the likelihood of unauthorised processing. It also prevents platforms from employing invasive data practices and abusing their dominant position to process data outside the legal purview. By ensuring that dominant players cannot gain an advantage through unfair data processing, this provision aims to level the playing field by mandating that all entities adhere to the same standards for data processing. As illustrated, mandating the processing of data only for lawful purposes, fosters competitive markets and safeguards user privacy. Consequently, there is no need for regulators to intervene, no requirement for regulatory coordination between the two regulators, and no recommended changes in either law.

A '**Level 2**' classification is assigned when a provision in either law has adverse impacts on both competition and data protection. For instance, consider the acquisition of a smaller company by a dominant firm with a similar data-driven business model. This scenario could result in increased data concentration, which negatively affects competition as a few entities control a significant portion of market data. This concentration could encourage monopolistic practices, hindering fair competition and innovation. Additionally, data concentration raises the risk of surveillance and security breaches, thereby hindering data protection and privacy efforts. Considering the impact of data-driven acquisitions on both competition and data protection, a minor change is suggested in the competition law to mandate the competition regulator to assess acquisitions based on data concentration. In this scenario, there is no ambiguity regarding which regulator should intervene, as this falls within the purview of the competition regulator.

A '**Level 3**' classification is assigned when a company's actions have a negative effect on both competition and data protection. This creates regulatory ambiguity due to uncertainty about the role of each regulator in resolving conflicts. Drawing from a previous example, Google implemented algorithmic changes to its search results, prioritising its own products and services over competitors and external websites, thereby adversely affecting market competition. Google's ability to manipulate search results raised questions about the nature and extent of data processing involved, leading to concerns about data privacy. In this situation, Google's actions have negative implications on both competition and data protection. While no changes are recommended in either law, a formal consultative process is recommended that would help establish a coordination mechanism between the CCI and the DPB to resolve the conflict in a joint consultative manner.

A '**Level 4**' classification is given when a provision (or lack thereof) in either law has a negative effect on data protection and a positive effect on competition or vice versa. For instance, the DPDP Act no longer has a provision for data portability. The absence of this provision decreases individual user control over data and prevents users to freely switch between services. This could potentially have a positive effect on competition as portability of data and access to datasets could help new market entrants build new products and services, as users could easily transfer their data from one data-holder to another. A data portability clause could also have a positive effect on competition by encouraging businesses to increase efficiency and regulate prices to retain customer loyalty. Introducing a data portability clause through an amendment of the data protection law could resolve a potential conflict of competing interests on privacy and competition that may arise from the lack thereof of such a provision.

A '**Level 5**' classification is assigned when a provision in either law has a contradictory effect, benefiting one aspect (either data protection or competition) while negatively impacting the other. In such cases, resolving the conflict falls outside the purview of both the DPB and the CCI. Instead, the courts must adjudicate the matter, considering the unique circumstances of the dispute. This approach is necessary to prevent amendments to legislation from undermining the core objectives of each fundamental law. For example, consider a dominant player in a data-driven market operating with limited competition. In this scenario, the CCI may intervene to mandate data interoperability between similar firms in the market. This mandate could address issues related to network effects by enabling smaller firms to access data held by the dominant player. However, it also raises concerns about data sharing with third parties without users' consent at the time of collection. Furthermore, mandating interoperability may compromise data security, particularly if it requires connecting a secure encrypted network with one of the lower security standards. Given the conflicting impacts on competition and data protection and the limitations in incorporating provisions in either legislation to alter the outcome, the courts must intervene to determine a resolution based on the specific context of the case.

Table 2: Level of conflict classification

Level of classification	Outcome	Effect on Competition	Effect on Data Protection	Recommended changes
Level 1	No conflict	Positive effect	Positive effect	No change is recommended in either law. Regulators do not need to intervene.
Level 2	No conflict	Negative effect	Negative effect	Minor change is recommended in either law.
Level 3	Conflict	Negative effect	Negative effect	Recommend that regulators set up a mechanism to coordinate a decision. A formal consultative process could be set up by signing a memorandum of understanding.
Level 4	Conflict	Positive effect	Negative effect	Recommend changes in either the law or the operating framework of each regulator.
		Negative effect	Positive effect	
Level 5	Conflict	Positive effect	Negative effect	Fundamental conflict cannot be resolved through changes in either law as it risks defeating the purpose of the specific law. Recommend courts to resolve the conflict on a contextual basis.
		Negative effect	Positive effect	

Source: Authors' analysis based on secondary research

Table 3: Impact on data security and competition objectives

	Specific example	Effect on Data Protection for Citizens	Effect on Competition in the Market	Level of classification
1	Processing data for lawful purposes	Positive effect on data protection: Greater user autonomy over data shared with data fiduciaries.	Positive effect on competition: All firms adhere to the same standards for data processing, levelling the playing field.	Level 1
2	Mergers and acquisitions in data-driven markets	Negative effect on data protection: Increased risk of surveillance and security breaches.	Negative effect on competition: Increased risk of data concentration.	Level 2
3	A big tech platform manipulating search results to benefit platform players	Negative effect on data protection: Potential unlawful processing of data.	Negative effect on competition: Products and services of dominant players are favoured over smaller competitors.	Level 3
4	Absence of data portability provision	Negative effect on data protection: Decreased user control over personal data.	Negative effect on competition: Raises barriers to entry and limited consumer choice risks decreasing innovation.	Level 4
5	Mandating data interoperability to facilitate competition	Negative effect on data protection: Potential to compromise data security.	Positive effect on competition: Decreasing the potential impact of network effects.	Level 5

Source: Authors' analysis based on secondary research

Conclusion

Based on existing literature regarding regulatory conflicts in India, this paper delineates the primary causes of such conflicts and their ramifications on regulators, regulated entities, and the market. It further examines the potential for similar conflicts between the CCI and the Data Protection Board concerning individual data rights and competition, classifying conflicts based on their level of severity. To decrease the likelihood of regulatory conflicts, we propose three recommendations:

1. **Role clarity**: When establishing regulators, responsibilities are often delineated without clear boundaries or directives. To mitigate ambiguity in their specific roles, objectives, and functions, it's essential to clearly define these aspects in the supporting legislation. Accountability and transparency mechanisms should be instituted to ensure that regulators are held accountable and to high standards. This approach will also help guarantee that each regulator adheres to its distinct roles and responsibilities. For instance, in the case of the Data Protection Board, determining whether there are 'sufficient grounds' to proceed with an inquiry made by a Data Principal necessitates establishing clear standards for such determinations. This clarity is crucial to avoid ambiguity and uphold fairness across cases.

2. **Minimise overlapping jurisdictions**: A primary factor contributing to regulatory conflicts in India is ambiguous legislative language, resulting in overlapping jurisdiction and blurred distinctions between two distinct regulators. When drafting legislation, it's crucial to consider the roles of other regulators in the market to prevent conflicting or competing functions. In cases of legislative overlap, updating the legislation to provide regulators with guidance on making necessary tradeoffs to resolve disputes is essential. For instance, the Delhi Electricity Commission claimed jurisdiction over the electricity sector regarding anti-competitive practices, while the CCI has jurisdiction over competition across all sectors. Including specific directives, such as determining which regulator should examine a case first, could guide resolution, prevent matters from escalating to the courts, and save significant time and money.

3. **Formal and institutionalised coordination mechanism**: In the instance of a regulatory conflict, there should be a formal and legislatively structured coordination mechanism that facilitates effective coordination between the regulators. It should effectively map out the distinct roles, responsibilities, and accountability of each regulator.[26] To uphold this process, there should be the establishment of a central coordination regulator that would ensure regulators are able to lead a coordinated effort to resolve a dispute. A “Central Regulatory Coordination Body” would function as the quality control and management system for a country’s regulatory process and regulations.[27] Canada, Chile, Colombia, El Salvador, Mexico, Peru, and the U.S. have instituted central coordination regulators and have seen greater inclusion of public opinion and

[26] To read more about regulatory coordination, please read this article.
[27] To learn more about Central Regulatory Coordination, please read this.

advancements in key areas of the national priorities.[28] In India, the establishment of a central regulatory body could streamline the resolution process and conserve time and resources of the courts while upholding the integrity of the markets.

The paper provides an overview of past regulatory battles in India and the mechanisms used to resolve these conflicts. Given the lack of coherent mechanisms in the past, it outlines the need for effective means to resolve conflicts. Implementing role clarity and minimising overlapping jurisdictions aims to decrease the likelihood of conflicts. However, even with efficient implementation, regulatory conflicts may still occur. Therefore, the paper focuses on enforcing mechanisms of coordination and cooperation between regulators. Ultimately, it emphasises the importance of balancing competition and data protection considerations to reach an optimal outcome that allows markets to function competitively while protecting user privacy.

[28] To learn more about the Central Regulatory Coordination Bodies in the above listed countries, please read this.

References

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). The consumer-data opportunity and the privacy imperative. *Mckinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Bundeskartellamt. (2016). Competition Law and Data. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2

Bundeskartellamt. (2019). Bundeskartellamt prohibits Facebook from combining user data from different sources. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

Burman, A. (2023). Understanding India's New Data Protection Law. *Carnegie India*. https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624

Central Regulatory Coordination Bodies. Inter-American Coalition for Regulatory Convergence. https://www.interamericancoalition-medtech.org/regulatory-convergence/quick-links/central-regulatory-coordination-bodies/

Central Regulatory Coordination. Inter-American Coalition for Regulatory Convergence. https://www.interamericancoalition-medtech.org/regulatory-convergence/policy/good-regulatory-practices/central-regulatory-coordination/#:~:text=A%20central%20coordinating%20body%20ensures,through%20its%20independence%20and%20expertise

Cho, S. (2023). A Study on the Regulation of Data Exploitative Conducts by Online Platforms under Competition Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4566575

Damodaran, S. (2009). Structured coordination of regulators. *The Economic Times*. https://economictimes.indiatimes.com/opinion/et-commentary/structured-coordination-of-regulators/articleshow/5248828.cms

Dey, S. (2013). RBI, CCI to vet all banking mergers. *Business Standard*. https://www.business-standard.com/article/finance/rbi-cci-to-vet-all-banking-mergers-112111900036_1.html

Diker, A., & Ünver, MB. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*. https://www.ejlt.org/index.php/ejlt/article/download/546/726?inline=1#_ftnref28

Draft Amendment to the Consumer Protection (E-Commerce) Rules, 2020. https://prsindia.org/billtrack/draft-amendments-to-the-consumer-protection-e-commerce-rules-2020

Grunes, A., & Stucke, M. (2015). No Mistake about it: The Important Role of Antitrust in the Era of Big Data. *University of Tennessee Legal Studies*. http://ssrn.com/abstract=2600051

Huddleston, J. (2021). The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More. *American Action Forum*. https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/

Interactions between Competition Authorities and Sector Regulators- Contributions from India. (2023). *OECD*. https://one.oecd.org/document/DAF/COMP/GF/WD%282022%2916/en/pdf

Interactions between Competition Authorities and Sector Regulators. (2022). *OECD Competition Policy Background Note*. https://web-archive.oecd.org/2022-10-25/643985-interactions-between-competition-authorities-and-sector-regulators-2022.pdf

Johnson, G., Shriver, S., & Goldberg, S. (2020). Privacy & market concentration: Intended and unintended consequences of the GDPR. https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-garrett_johnson.pdf

Kerf, M., Neto, I., & Geradin, D. (2005). Antitrust vs. Sector Specific Regulation in Telecom: The Impact on Competitiveness. *Social Science Research Network*. https://doi.org/10.2139/ssrn.886316

Khan, L. (2017). Amazon's antitrust paradox. *Yale Law Journal*.

Kumar, V., & Singh, P. (2021). India's competition laws need to tackle regulatory shopping. *East Asia Forum*. https://eastasiaforum.org/2021/05/21/indias-competition-laws-need-to-tackle-regulatory-shopping/

McCabe, D., & Mickle, T. (2024). U.S. moves closer to filing sweeping antitrust case against Apple. *The New York Times*. https://www.nytimes.com/2024/01/05/technology/antitrust-apple-lawsuit-us.html

Mills, K. (2022). Consent and the right to privacy. *Journal of Applied Philosophy*. https://doi.org/10.1111/japp.12592

Mishra, R. (2013). Harmonising Regulatory Conflicts. *CUTS Institute for Regulation and Competition*. https://www.cuts-ccier.org/pdf/Harmonising_Regulatory_Conflicts.pdf

Nuccio, M. (2017). Contestable markets and price discrimination in data-driven businesses. *Nexa Center for Internet & Society Politecnico di Torino*. https://nexa.polito.it/nexacenterfiles/2-Nuccio-contestable-markets.pdf

Paul, P. Conflicts of jurisdiction between SEBI and other regulators. *Indian Law Journal*. https://www.indialawjournal.org/archives/volume7/issue-2/article6.html

Radinsky, K. (2015). Data Monopolists Like Google Are Threatening the Economy. *Harvard Business Review*. https://hbr.org/2015/03/data-monopolists-like-google-are-threatening-the-economy

Recurring Jurisdictional Turf -war between CCI and Sectoral Regulators. (n.d.). *CUTS Institute for Regulation and Competition*. https://cuts-ccier.org/newsletter/spotlight-15.htm

Robb, L., Candy, T., & Deane, F. (2022). Regulatory overlap: A systematic quantitative literature review. *John Wiley & Sons Australia*. https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/rego.12504

Rubinfeld D., & Gal, M.S. (2017). Access barriers to Big Data. *Arizona Law Review*. https://cris.iucc.ac.il/en/publications/access-barriers-to-big-data

Schepp, N.P., & Wambach, A. (2015). Competition policy: The challenge of digital markets. *German Monopolies Commission (Monopolkommission)*. http://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf

Securities and Exchange Board of India Act, 1992. (1992). https://www.sebi.gov.in/sebi_data/attachdocs/1456380272563.pdf

Sinha, V., & Srinivasan, S (2021). An integrated approach to competition regulation and data protection in India. CSI Transactions on ICT. 9(3), 151–158. doi:10.1007/s40012-021-00334-7

The Digital Personal Data Protection Act, 2023. (2023). Bill No. 384, The Digital Personal Data Protection Bill, Vol. 1. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

The Digital Personal Data Protection Act, 2023. (2023). Bill No. 384, The Digital Personal Data Protection Bill, Vol. 1. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

The Electricity Act, 2003. (2003). https://cercind.gov.in/Act-with-amendment.pdf

The governance of regulators. (2014). *OECD Best Practice Principles for Regulatory Policy*. https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page4

The Petroleum and Natural Gas Regulatory Board Act, 2006. (2006). https://lddashboard.legislative.gov.in/sites/default/files/A2006-19.pdf

The Regional Rural Banks Act, 1976. (1976). https://www.indiacode.nic.in/bitstream/123456789/1492/1/197621.pdf

The Reserve Bank of India Act, 1934. (1934). https://www.indiacode.nic.in/bitstream/123456789/2398/1/a1934-2.pdf

The Telecom Regulatory Authority of India Act, 1997. (1997). https://trai.gov.in/sites/default/files/The_TRAI_Act_1997.pdf