CRITICAL ANALYSIS ON THE INTERFACE BETWEEN INDIAN DIGITAL DATA PROTECTION ACT & PROPOSED DIGITAL COMPETITION BILL

Sameer Mishra
College Student
Amity Law School and College
Amity University, Noida, India
sam16mishra@gmail.com

Abstract

The swift advancement of India's digital economy entails a closer examination of how data protection and anti-trust laws intersect. This paper explores the interface between India's Digital Personal Data Protection Act, 2023 (DPDPA) and its anti-trust laws regime, namely the Competition Act of 2002 and the proposed Digital Competition Bill, 2024 (DCB). This paper analyses the role of Private Data as a pivotal competitive asset in digital markets, raising concerns at the nexus of privacy and competition. Through a doctrinal analysis, we review relevant literature and jurisprudence, including an OECD working paper and scholarly contributions, to understand global perspectives on the competition privacy interface. This is followed by a comprehensive legal scrutiny of the Indian frameworks, coupled with case studies of recent landmark decisions by the Competition Commission of India (CCI), in particular, CCI's orders against Google (Android licensing and Play Store billing) and Meta (WhatsApp's 2021 privacy policy). A comparative jurisprudential lens is applied, examining the European Union's approach (Article 102 TFEU, the Digital Markets Act (DMA), and the German Meta case) to highlight convergent trends and lessons for India. The analysis reveals significant areas of overlap between privacy and competition regulation, for instance, how misuse of user data by dominant firms can both violate privacy rights and harm competition, as well as gaps where neither regime alone adequately safeguards consumer welfare. Finally, the Paper offers policy recommendations for harmonizing data protection and antitrust enforcement in India's digital economy. The Paper advocates for cooperative regulatory mechanisms and calibrated reforms to address data as a competitive asset while protecting individual privacy, thereby ensuring innovation, fair competition, and user safety in the digital age.

Objectives of the Study:

Main objectives of this dissertation are:

1. To examine the substantive provisions of the DPDPA, 2023 and the Digital Competition Bill, 2024.
2. To analyse the interface between privacy protection and competition regulation in the context of digital markets.
3. To identify potential areas of overlap, conflict, and synergy between the two legal frameworks.
4. To evaluate how regulatory frameworks in other jurisdictions have managed similar overlaps.
5. To recommend a coherent and harmonized regulatory approach for India.

Research Methodology:

The research adopts a doctrinal legal methodology with comparative and analytical dimensions. Primary sources include the statutory texts of the DPDPA 2023, the Digital Competition Bill 2024, relevant case law, committee reports, and legislative debates. Secondary sources include scholarly articles, think tank reports, and comparative jurisprudence from the EU, US, and UK.

This dissertation also includes case studies involving tech giants like Google, Meta, and Amazon to illustrate how data-driven dominance raises dual concerns of privacy infringement and market distortion.

The study does not rely on empirical or quantitative data but emphasizes a normative, legal, and policy analysis grounded in principles of constitutional law, regulatory theory, and market economics.

Chapter 1: Introduction

Digital economy of India has undergone a remarkable transformation over the years, positioning the nation as a leader in digital revolution and connectivity. As of early 2025, India is home to over 806 million internet users, representing a penetration rate of approximately 55.3% of its 1.46 billion population[1]. Projections suggest this figure will exceed 900 million by the end of 2025, driven by the increasing availability of affordable smartphones and data plans[2]. The widespread adoption of smartphones, with estimates indicating around 659 million users in 2025,[3] has been a key catalyst, enabling access to digital services across urban and rural areas. Steps taken by the government like Digital India have further accelerated this growth by encouraging digital learning and infrastructure development, particularly in underserved regions[4].

The economic impact of this digital surge is profound. In 2022-23, the digital economy contributed approximately 11.74% to India's national income, equivalent to INR 31.64 lakh crore (roughly US$ 402 billion), encompassing digital-enabling industries like information & communication technology, new digital platforms, and digital contributions from traditional sectors[5]. Reports indicate that by 2030, this contribution could approach 20% of national income, growing nearly twice as fast as the overall economy[6]. Sectors such as e-commerce, in 2024 valued at $147.3 billion with an 18.7% compound annual growth rate (CAGR) over 2028,[7] and fintech, driven by innovations like the Unified Payments Interface (UPI), are at the forefront of this expansion. The digital economy also supports 14.67 million jobs, representing 2.55% of India's workforce, underscoring its role in employment generation.

[1] DataReportal, "Digital 2025: India," accessed April 18, 2025, https://datareportal.com/reports/digital-2025-india.

[2] India Brand Equity Foundation, "India's Internet Users to Exceed 900 Million in 2025, Driven by Indic Languages," accessed April 18, 2025.

[3] GrabOn India, "Smartphone Usage Statistics & Trends in 2025," accessed April 18, 2025, https://www.grabon.in/indulge/tech/smartphone-usage-statistics/

[4] India Brand Equity Foundation, "The Digital India Programme: Transforming Nation," accessed April 18, 2025, https://www.ibef.org/government-schemes/digital-india.

[5] Ministry of Electronics and Information Technology, "Estimation and Measurement of India's Digital Economy," accessed April 18, 2025, https://www.meity.gov.in/writereaddata/files/Report_Estimation_Measurement.pdf.

[6] Anirudh Burman and Pronab Sen, "Digital Economy to Constitute Fifth of Indian GDP by 2030: ICRIER Report," The Hindu, December 16, 2024, https://www.thehindu.com/business/digital-economy-to-constitute-fifth-of-indian-gdp-by-2030-icrier-report/article69131201.ece

[7] "Internet in India," Wikipedia, last modified April 15, 2025, https://en.wikipedia.org/wiki/Internet_in_India

This rapid digitalization, while a boon for economic growth and innovation, has introduced significant regulatory challenges. The vast volume of personal data generated by digital platforms raises critical concerns about privacy and security. High-profile data breaches and instances of unauthorized data sharing have heightened civic cognizance of the need to safeguard individual privacy rights, recognized as a fundamental right under the 2017 Puttaswamy judgment[8]. Concurrently, the dominance of a few large technology companies has led to market concentration, potentially stifling competition and innovation. For example, decision of the Competition Commission of India (CCI) in WhatsApp's 2021 privacy policy update case revealed how data-sharing practices can impact market competition, while allegations against Amazon for leveraging non-public seller data highlight the risks of abuse by dominant entities in digital markets. These cases illustrate the intricate relationship among data protection and competition laws, necessitating a cohesive regulatory approach.

To address these challenges, India has introduced a trio of legislative frameworks. On one hand is the framework for data protection and privacy rights, which has culminated in the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA). The DPDPA – India's first cross-sectoral data protection legislation – was enacted after extensive deliberation and multiple draft iterations, reflecting the nation's response to the case of *Justice K.S. Puttaswamy v. Union of India (2017)*[9]. It establishes rights for individuals (data principals) and responsibilities for entities handling personal data (data fiduciaries), with an emphasis on user consent, lawful and minimal data processing, and accountability through a new Data Protection Board. On the other hand, is India's competition law regime under the Competition Act, 2002, enforced by the Competition Commission of India (CCI). The CCI has been active in scrutinizing digital markets to prevent abuses of dominance and anti-competitive agreements. Traditional competition law tools – addressing issues like exclusive contracts, tying arrangements, self-preferencing, predatory pricing, etc. – are being tested and expanded in the context of digital platforms that thrive on network effects and data aggregation.

In addition, a Committee on Digital Competition Law recently proposed an ex-ante regulatory regime for large digital players, resulting in the draft Digital Competition Bill, 2024 (DCB)[10]. The DCB seeks to designate certain major online platforms as "Systemically Significant Digital Enterprises (SSDEs)" and impose upon them a set of pro-competitive obligations (similar in spirit to the EU's Digital Markets Act). These comprise embargoes on self-preferencing, anti-steering, tying, and misuse of data practices through which dominant digital firms could unfairly cement their market power. The DCB thus explicitly acknowledges that control over data can be a source of anti-competitive conduct.

The Digital Personal Data Protection Act, 2023 (DPDPA) establishes a comprehensive data privacy regime, emphasizing user consent, data minimization, and the creation of a Data Protection Board (DPB) to oversee compliance. The Competition Act, 2002, enforced by the CCI, seeks to promote fair competition by preventing agreements that are anti-competitive, abuse of dominance, and harmful mergers. The proposed Digital Competition Bill, 2024 (DCB) introduces ex-ante regulations targeting Systemically Significant Digital Enterprises (SSDEs), aiming to pre-empt anti-competitive behaviour through measures like data portability and interoperability mandates.

These frameworks intersect on critical issues such as data sharing, market power, and consumer welfare, but their differing objectives may lead to tensions. For instance, the DCB's push for data sharing to enhance competition could conflict with the DPDPA's stringent consent requirements, creating compliance dilemmas for digital platforms. Similarly, the designation of Significant Data Fiduciaries under the DPDPA may overlap

[8] 2017 INSC 801

[9] **PRS Legislative Research. (2023).** *Digital Personal Data Protection Bill, 2023*. PRS India. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#:~:text=Personal%20data%20is%20information%20that,loss%20of%20reputation%2C%20and%20profiling

[10] **Ministry of Corporate Affairs. (2024).** *Report of the Committee on Digital Competition Law and Draft Digital Competition Bill*. Government of India. https://www.mca.gov.in/bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open

with the CCI's oversight of dominant firms, raising questions about jurisdictional clarity. Resolving these tensions is essential to ensure that India's digital economy remains vibrant, competitive, and trustworthy.

The global context offers valuable insights for navigating these challenges. The European Union (EU) has been a pioneer in dealing with digital markets and data protection through the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA). The GDPR's robust privacy protections and the DMA's proactive regulation of gatekeeper platforms provide a model for balancing consumer rights with market fairness. By examining the EU's approach, India can identify best practices and potential pitfalls, informing the development of its regulatory framework.

This paper aims to explore the interface between the DPDPA, the Competition Act, and the proposed DCB, analyzing their synergies, conflicts, and implications for India's digital economy. Through detailed case studies, such as the CCI's investigations into WhatsApp and Amazon, the paper will illustrate the practical application of these laws. A comparative analysis with the EU's GDPR and DMA will highlight global perspectives, offering lessons for harmonizing India's regulatory approach. Ultimately, the paper aims to propose strategies that balance the imperatives of data protection and fair competition, fostering an innovative, inclusive, and consumer-centric digital ecosystem in India.

1.1: Literature Review

Early scholarship on privacy and competition law treated these two domains as largely separate spheres serving different objectives: data protection laws focus on individual autonomy and privacy rights, whereas competition laws aim to preserve market efficiency and consumer welfare (often measured in price, quality, and innovation). Traditionally, competition regulators were reluctant to treat privacy concerns as part of their mandate, adhering to the view that a firm's misuse of personal data (for example, violating users' privacy expectations) did not directly pertain to competition unless it involved exclusionary conduct or higher prices. However, as digital markets evolved, this strict separation has been increasingly questioned. Scholars and policymakers observed that in "free" online services where consumers pay with their data and attention rather than money, privacy can be used as a milestone of product quality. If a dominant firm reduces the privacy protections it offers (e.g., by intensive personal data collection or sharing without consent), users experience a deterioration in quality, analogous to a price increase in terms of welfare effects[11]. Thus, a reduction in privacy can constitute a form of consumer harm in competition analysis.

International policy bodies have also examined the connection between anti-trust and data privacy. A 2024 policy paper by the Organisation for Economic Co-operation and Development (OECD) emphasizes that data has become central to competitive advantage in digital markets, particularly as privacy regulations continue to proliferate globally.[12] The paper raises critical questions regarding whether the collection of consumer data constitutes an antitrust concern and, conversely, whether competition deliberations should influence data protection enforcement. It highlights that certain digital business models rely heavily on extensive personal data collection often described as "commercial surveillance" which may simultaneously contribute to market power and infringe on individual privacy. There is increasing recognition that these two regulatory domains are interrelated and that cooperative strategies between them should be developed. Notably, the paper

[11] **Gorecka, A. (2024).** *On the interplay between competition law and privacy: The impact of Meta Platforms case*. European Competition Journal. https://pure.strath.ac.uk/ws/portalfiles/portal/250673473/Gorecka-ECJ-2024-On-the-interplay-between-competition-law-and-privacy.pdf

[12] Organisation for Economic Co-operation and Development. (2024). *The intersection between competition and data privacy*. https://www.oecd.org/daf/competition/the-intersection-between-competition-and-data-privacy.pdf

concludes that institutional mechanisms fostering co-operation between competition and data protection authorities are necessary, especially as an increasing number of cases touch upon both sets of issues.

Not all commentators, however, fully embrace the convergence of privacy and competition enforcement. Some warn of the dangers of "mission creep" in antitrust enforcement. They argue that competition authorities lack the expertise to adjudicate data protection issues and that stretching antitrust to cover privacy could lead to incoherent outcomes or double jeopardy for firms. For example, a critique by Bal (2024) of the CCI's WhatsApp order (discussed later) terms it "experimental antitrust" and finds doctrinal inconsistency in the way the CCI combined privacy and competition rationales[13]. The concern is that regulators might prohibit conduct without clear evidence of traditional competition harm, simply because it offends privacy norms – thereby moving away from established competition law principles. Such critiques underscore the need for a principled framework when addressing overlap cases: competition intervention should be grounded in competition logic (e.g. how the privacy-invasive conduct harms the competitive process or consumer welfare in the market), even if it concurrently violates privacy standards.

Overall, the literature reflects a paradigm shift: data and privacy are now recognized as integral to market competition in the digital age. There is broad agreement that strong privacy protections and robust competition can complement each other in empowering consumers – for instance, more competition can incentivize firms to offer better privacy options, and stronger privacy law (like data portability rights) can lower barriers to switching, enhancing competition. At the same time, scholars emphasize careful calibration: regulators should coordinate to avoid conflict (so that a company isn't caught between contradictory mandates), and should leverage each other's strengths (for example, using privacy law to set baselines for data handling and competition law to tackle market power issues arising from data). The next sections build on these insights to assess India's approach in its new privacy law and competition enforcement, evaluating how the interplay is unfolding in practice.

1.2: Background and Context:

In the age of digitization, data has emerged as the currency of the 21st century. From personalized advertising to algorithmic decision-making, the centrality of data to business models and digital services has prompted a wave of legislative reforms worldwide. India, with its burgeoning digital economy and a population of over 1.4 billion, is at the forefront of this digital transformation. Amid increasing concerns around data misuse, privacy, algorithmic biases, and market power concentration, two significant legal frameworks have emerged on the Indian legislative horizon, the **Digital Personal Data Protection Act, 2023** (DPDPA) and the **Digital Competition Bill, 2024**.

The DPDPA 2023 is first Indian data protection legislation, rooted in the principles of informed consent, purpose limitation, and user empowerment. On the other hand, the Digital Competition Bill, 2024, proposes to amend the existing Competition Act, 2002, with a renewed focus on digital markets, particularly targeting dominant digital platforms and gatekeeper behaviour.

While these legislations operate in different domains, privacy and competition, their interface is both inevitable and critical. The growing dominance of data-rich digital firms has blurred traditional lines between consumer protection, privacy, and fair competition. As data becomes an economic asset and a strategic resource, its collection, use, and control are increasingly being scrutinized not just from a privacy standpoint, but also from the lens of market fairness and anti-competitive conduct.

[13] **Bal, M. (2024, November 26).** *The CCI's order in the WhatsApp privacy policy case highlights the perils of regulators engaging with experimental antitrust*. Esya Centre. https://www.esyacentre.org/perspectives/2024/11/26/the-ccis-order-in-the-whatsapp-privacy-policy-case-highlights-the-perils-of-regulators-engaging-with-experimental-antitrust

Chapter 2: Legal Analysis: Digital Personal Data Protection Act, 2023 and Its Proposed Rules

2.1: Overview of the DPDPA

The Digital Personal Data Protection Act (DPDPA), 2023[14], passed in August 2023, is India's first cross-sectoral legislation on personal data protection, finalized after varied discussions for more than half a decade. The Act represents the culmination of several iterations, beginning with a 2018 draft by the Srikrishna Committee and evolving through subsequent drafts in 2019, 2022, and finally the 2023 version. This progression reflects India's response to the growing need for safeguarding individual privacy, as recognized in the landmark 2017 judgment (*Justice K.S. Puttaswamy v. Union of India*), which established privacy as a fundamental right.

The earlier 2019 draft proposed a preventive regulatory framework emphasizing stringent data protection measures, such as categorizing personal data into sensitivity levels, introducing consent managers, and imposing obligations on data fiduciaries like data audits and impact assessments. It also proposed a powerful Data Protection Authority to oversee compliance, raising concerns about the potential for overregulation. However, the expansive scope and heavy compliance burdens of the 2019 draft drew criticism, particularly from businesses.

In contrast, the 2023 Act, largely based on the 2022 draft, takes a simplified approach, streamlining the regulatory framework while focusing on individual rights and lawful processing of personal data. This evolution reflects a shift from the preventive stance of earlier drafts to a more flexible framework that balances the private rights of a person and the practical needs of businesses. By reducing the regulatory burden, the DPDPA aims to foster innovation while safeguarding data protection, setting the stage for further growth of data protection norms in India.

2.2: Key highlights of the DPDPA

The DPDPA demonstrates an outline for regulating the collection, storage, and processing of digital personal data, balancing individuals' rights with the legitimate interests of entities processing data. Key provisions include:

1. **Applicability**: The Digital Personal Data Protection Act (DPDPA) applies specifically to personal data that is either collected in digital form or converted into digital format from non-digital sources. Its applicability extends beyond India, which covers the processing of data which are conducted outside the country when it refers to offering goods or services to entities in India. However, the Act ignores personal data processed for purely personal or internal purposes, as well as data that individuals have voluntarily made public or disclosed under legal obligations.

2. **Uniform Treatment of Data**: The DPDPA does not differentiate among the categories of individual data such as sensitive, critical. This uniform approach contrasts with earlier frameworks that prescribed varying compliance standards for different types of data.

3. **Consent-based Data Processing**: The DPDPA mandates that the data processing consent must remain affirmative, meaning it should be clear, specific, informed, and voluntarily provided through an

[14] **Government of India.** (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Gazette of India. April 18, 2024, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

unambiguous action. Individuals have the right to withdraw the permission as easily as they provided it, without impacting the legality of processing conducted before withdrawal. Organizations are required to provide a mandatory notice to individuals, outlining the aim of collection of the data, their rights, and the available grievance mechanisms. To ensure accessibility, notices and consent, forms must be presented in English and in other languages as listed in the Eighth Schedule of the Constitution of India. Additionally, the Act permits data processing without explicit consent in specific scenarios, such as performing state functions, addressing medical emergencies, or complying with legal obligations.

4. **Data Protection Principles**: The DPDPA emphasizes key data protection principles to ensure responsible data handling. It mandates that personal data must be managed strictly for legal purposes that align with the consent of the individual, adhering to the principle of purpose limitation. Additionally, under the principle of collection limitation, data collection is restricted to only what is essential to achieve the stated purpose, avoiding excessive or irrelevant data gathering.

5. **Data Fiduciaries**: Data fiduciaries are obligated to ensure compliance with the provisions of the DPDP Act, comprising any private data processing carried out by data processors on their behalf. When handling personal data that could influence decisions affecting the data principal or is intended for sharing with another fiduciary, they must ensure the data's accuracy and completeness. Additionally, the personal data must be deleted by the fiduciaries when the data principal withdraws permission or when the intended aim is reasonably deemed to be fulfilled, unless retaining the data is necessary to comply with legal obligations.

6. **Significant Data Fiduciaries**: The Central Government has the authority to designate some data fiduciaries as important, built on criteria like the volume and sensitivity of data handled, risks to individuals' rights, or concerns related to state security. These entities must fulfil additional responsibilities, which includes appointing an officer for protection of data located in India, which engages an independent inspector to evaluate compliance, and conducting regular audits and impact assessments. They are also required to implement other prescribed measures to ensure robust data protection practices.

7. **Rights of Data Principals**: Under the DPDP Act, data principals are granted a range of rights to ensure control on their private data. Individuals are granted privileges like data contact, correction, portability. Further, they got the ability to look into the detailed information about their data, such as summaries of ongoing processing activities and identities of entities the data was shared. Additionally, data fiduciaries are required to provide accessible mechanisms for addressing grievances, which data principals must utilize fully before escalating matters to the Data Protection Board.

8. **Establishment of Data Protection Board (DPB)**: The DPDP Act envisions the creation of the Data Protection Board (DPB) to serve as a regulatory authority with enforcement capabilities. The DPB is empowered to take immediate corrective actions in response to reported data breaches, conduct investigations, levy fines for violations, review documents, and summon individuals as necessary. Choices that are made by the DPB can get challenged before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within a specified timeframe.

2.3: Proposed DPDP Rules:

One important aspect of the DPDPA is that it is designed as an "umbrella legislation" with many details to be fleshed out in subordinate Rules. The proposed DPDP Rules, 2025, published on January 3, 2025, and is open for community discussion until February 18, 2025, provide a detailed framework for implementing the

DPDPA[15]. These rules introduce specific obligations for Significant Data Fiduciaries and establish the role of Consent Managers, both of which have significant implications for competition in India's digital economy.

2.4: Significant Data Fiduciaries (Rule 12)

Significant Data Fiduciaries are entities advised by the Central Government built on criteria like the volume of private information processed, the influence on the economy, or the risk to data principals. For example, e-commerce platforms with over 20 million users might be classified as Significant Data Fiduciaries. Significant Data Fiduciaries must conduct DPIAs and audits every 12 months to assess compliance with the DPDPA and identify risks to data principals. These assessments ensure robust data governance but impose significant administrative and financial burdens. Fiduciaries must verify that algorithms used for processing personal data (e.g., in hosting, publishing, or sharing data) do not infringe on data principals' rights, addressing concerns about automated decision-making.

2.5: Consent Managers (Rule 4 and First Schedule)

Consent Managers are Indian companies acting as intermediaries, enabling users to manage consent across platforms via interoperable systems. They operate as intermediaries, allowing data bodies to give, manage, review, and withdraw permission via interoperable platforms. They require a minimum net worth of INR 2 crore, robust technical capacity, and DPB registration. They must ensure data confidentiality, maintain seven-year consent records, and operate transparently with regular audits. They apply for registration with the DPB, which may approve, reject, or suspend their status based on compliance. Consent Managers provide platforms (e.g., websites or apps) for users to manage consent across multiple Data Fiduciaries. For example, a user could use a Consent Manager to authorize data sharing between a bank and a fintech platform, ensuring transparency and control.

Crucially, nothing in the DPDPA explicitly addresses competition or market power issues its focus is individual rights and data handling obligations. Yet, indirectly, its provisions (or absence thereof) can have competitive effects. For example, by not providing a data portability right, the Act does not itself empower users to easily transfer their data to a rival service (whereas GDPR's portability right could facilitate switching from one platform to another, reducing lock-in). Likewise, the DPDPA's emphasis on consent means a dominant digital firm can legally collect and use extensive personal data *so long as it obtains user consent*. But if consent is effectively a take-it-or-leave-it proposition (take use of the service or lose it), the question arises: is that consent truly "free" and valid? The Act and draft rules suggest consent tied to provision of service may be scrutinized – any unnecessary data collection bundled into a service agreement could be deemed not freely given[16]. However, unlike competition law, the DPDPA does not explicitly forbid making a service conditional on data sharing; it relies on the abstract concept of "free" consent. As we shall see, this is where competition law might step in to condemn such behaviour as "unfair" even if it squeaks by the consent requirement.

In summary, the DPDPA establishes a broad consent-centric privacy framework that empowers users, but it stops short of mandating data sharing or portability that could directly alleviate competitive concerns (except via general user-driven consent choices). Its successful enforcement (through the Data Protection Board) will be key to ensuring companies actually give effect to user autonomy. Weak enforcement could enable dominant firms to continue opaque or forceful data practices, whereas strong enforcement could curb exploitative data handling. This interplay with competition is considered in detail later with the WhatsApp case study.

2.6: Competition Act, 2002- Abuse of Dominance and the Rise of Data Concerns

The Competition Act of 2002, the primary antitrust statute of India, aimed at preventing the exercises which are having Appreciable Adverse Effect on Competition (AAEC), promoting user interests, and it makes sure

[15] https://innovateindia.mygov.in/dpdp-rules-2025/

[16] **International Association of Privacy Professionals. (2024, February 12).** *Decoding India's draft DPDPA rules for the world*. IAPP. https://iapp.org/news/a/decoding-india-s-draft-dpdpa-rules-for-the-world

that there is freedom to trade. For the purposes of this paper, the most relevant provisions are those dealing with Abuse of Dominant Position (Section 4 of the Act), given many digital market issues revolve around dominant firms exploiting their position. Section 4(1) prohibits any enterprise from abusing its dominant position. Section 4(2) provides an illustrative list of what constitutes abuse, including: (a) imposing unfair or discriminatory conditions or prices in the purchase or sale of goods or services, (b) limiting or restricting production of goods, provision of services or technical or scientific development to the prejudice of consumers, (c) indulging in practices resulting in denial of market access to competitors, (d) making the conclusion of contracts subject to acceptance of supplementary obligations unrelated to the contract (a form of tying), and (e) using dominance in one market to protect or leverage into another market. These broad categories map closely to classic antitrust theories of harm: exploitative abuse (unfair conditions/prices) and exclusionary abuse (foreclosure of competitors through tying, denial of access, leveraging, etc.).

Notably, Section 4 does not require proof of intent, it is effects-based, and the list is not exhaustive, meaning other conduct by a dominant firm that harms competition or consumers can also be deemed abusive. The Act thus provides the CCI considerable flexibility to characterize novel forms of behaviour as abusive, provided they can be shown to fit within the spirit of these categories. This flexibility has proven useful in digital market cases, where traditional price-based analyses often give way to considerations of non-price factors and platform ecosystem strategies.

Competition Act does not expressly mention "data" or "privacy" anywhere, as it was drafted at a time (early 2000s) when such issues were not forefront in antitrust discourse. However, its broad language (e.g., "unfair conditions" or "prejudice of consumers") leaves room for incorporating those considerations. For instance, one could argue that a dominant platform imposing a privacy-invasive term on users (such as mandatory data sharing with third parties) is imposing an "unfair condition" on sale of its service, thus violating Section 4(2)(a). Similarly, using data collected from users in one domain to gain advantage in another domain might be conceptualized as a form of leveraging dominance under Section 4(2)(e), if it can be framed as using dominance in market A to enter/protect position in market B.

Enforcement of the Act is entrusted to the Competition Commission of India (CCI), which has powers to conduct inquiries, impose penalties and issue cease-and-desist or behavioural orders, among other remedies. The CCI can also impose structural remedies (though rarely used so far) or direct modifications in conduct. The orders of any entity being dominant and the concern for data can be appealed in the National Company Law Appellate Tribunal (NCLAT) and if required then it can be appealed to the Supreme Court.

One vital feature of the Act in context of overlapping regulation is Section 62, which provides that the 2002 Competition Act is adding to, and not in condemnation of, any additional law in force. Meanwhile, Section 60 states that the Act intend to have result notwithstanding anything unreliable in any additional law. Read together, these mean that generally the Act is intended to coexist with other regulatory laws (like the DPDPA) and not override them, unless there is a direct inconsistency, in which case the Competition Act would prevail. So far, no direct inconsistency between a competition remedy and a privacy rule has arisen in India (partly because the DPDPA is very new). But these provisions suggest that, for example, if the Data Protection Board were to approve a certain conduct under DPDPA, it wouldn't automatically immunize that conduct from competition scrutiny if it harms competition; the CCI's mandate could still apply.

In the last few years, the CCI has dealt with numerous big-tech cases that underscore the importance of data as an element of competition analysis. For example, in defining relevant markets and assessing dominance, the CCI has cited factors like user base size, network effects, and access to data. In *Harshita Chawla vs WhatsApp (2020)*[17], a case concerning WhatsApp's alleged tying of its payments service to its messaging app, the CCI explicitly remarked that access to a large user data trove can confer competitive advantage. These instances

[17] **Competition Commission of India. (18.08.2020).** *[*Harshita Chawla vs. WhatsApp Inc.*]* (Case No. 15 of 2020). https://www.cci.gov.in/antitrust/orders/details/118/0

show that even before a formal data protection law was in place, the competition regulator was conscious of data's role.

The most direct integration of privacy considerations into competition analysis by CCI came in its recent *WhatsApp Privacy Policy* case (2021-2024), which we will analyze in detail later. There, the CCI treated WhatsApp's *lack of choice given to users over data sharing* as an "unfair term" of service and examined how that facilitated Meta's market power. This indicates a willingness on the CCI's part to protect not just competition in a structural sense but also consumers from exploitative conduct that has a data/privacy dimension.

2.7: Proposed Digital Competition Bill, 2024

Over the years, the unprecedented success and impact of Big Tech companies have triggered global concerns about their unchecked market power and the potential for anti-competitive behaviour. In response, governments and regulatory bodies worldwide have taken steps to establish frameworks to monitor and regulate digital markets. India has joined this global movement by taking proactive steps to address these issues through the Committee on Digital Competition Law (CDCL), established in 2023. The primary mandate of this committee was to evaluate the unique challenges posed by digital markets and assess the necessity for a dedicated legal framework to regulate competition in this space.

After extensive deliberations spanning more than a year, the CDCL submitted its report to the Ministry of Corporate Affairs (MCA) in March 2024. Alongside the report, it introduced the Digital Competition Bill, 2024 (DCB), which represents a significant shift in India's approach to competition law. After public consultation on the same, the Bill is currently under examination with MCA.

The DCB proposes an ex-ante regulatory framework, which aims to pre-emptively address anti-competitive practices rather than relying solely on traditional ex-post enforcement mechanisms. This forward-looking approach is tailored to the dynamic nature of digital markets, where traditional competition laws often struggle to keep pace with the rapid evolution of technology and business models. By establishing a proactive framework, the DCB seeks to mitigate potential harm to market fairness and consumer welfare before it occurs. The DCB focuses on regulating Systemically Significant Digital Enterprises (SSDEs) to ensure fairness, transparency, and contestability in digital markets. Key features include:

1. **Designation of SSDEs**: Under the DCB, the concept of Systemically Significant Digital Enterprises (SSDEs) plays a central role in ensuring fair competition within the digital economy. Enterprises that meet certain predefined financial and user thresholds—such as revenue, market capitalization, or user base size—will be designated as SSDEs. This designation reflects their significant market presence and influence in core digital services. The thresholds are structured to identify entities that hold substantial power in the market, potentially capable of engaging in anti-competitive practices that could harm competition, innovation, and consumer welfare.

2. **Self-Reporting**: The DCB establishes a self-reporting requirement for entities likely to qualify as SSDEs. Enterprises are mandated to notify the CCI within 90 days of crossing the specified thresholds, enabling the regulatory body to assess their status and enforce compliance. This self-reporting mechanism ensures that the process of designation is transparent and efficient, allowing the CCI to focus its oversight efforts on enterprises with the greatest potential to influence competition adversely.

3. **Oversight by CCI**: DCB entrusts the CCI with the critical responsibility of ensuring compliance with the regulatory obligations imposed on SSDEs. This oversight includes ensuring compliance with obligations under DCB *inter alia* including investigating anti-competitive behaviors such as self-preferencing, anti-steering, and the misuse of non-public data, etc.

4. **Obligations on SSDEs**: Once designated as an SSDE, these enterprises will be subjected to a set of tailored regulatory obligations aimed at curbing anti-competitive conduct and promoting market fairness. These obligations include prohibitions on practices like self-preferencing, anti-steering, and the unfair use of non-public data, ensuring transparency and accountability in their operations. By imposing these obligations, the DCB seeks to pre-emptively address market distortions that could arise due to the dominance of these enterprises. These obligations, enumerated in the DCB, echo many findings that the CCI made in ex post cases as well as obligations from the DMA. For example:

    - **Self-preferencing (Section 11):** An SSDE must not favor its own products or services over those of third-party business users on its platform. This tackles the issue of platform neutrality (e.g. an app store promoting its own apps in search rankings).

    - **Restrictions on third-party application installation (Section 13):** It cannot restrict users from installing or using third-party apps or services, and must allow users to choose defaults – addressing concerns like those in the Android case about pre-installation and default settings.

    - **Anti-steering (Section 14)**: It must not prevent business users from communicating with their customers or directing them to alternative channels (for instance, app developers should be free to tell users about other payment options).

    - **Tying and bundling (Section 15):** Prohibits forcing users to use an SSDE's other services as a condition for using the core service, unless absolutely necessary.

    - **Data usage constraints (Section 12):** This is most pertinent for our discussion. Section 12(1) of the DCB flatly prohibits an SSDE from using non-public data of its business users to gain competitive advantage against them. In essence, an e-commerce platform like Amazon (if designated) could not exploit the sales or inventory data of third-party sellers on its platform to launch or optimize Amazon's own competing products – a practice that had raised global antitrust ire. "Non-public data" is defined broadly to include any data generated by business users or their customers on the platform that isn't publicly available. Section 12(2) then targets the intermingling of personal data across services: an SSDE shall not *"without consent of end users or business users, intermix or cross-use the personal data collected from different services"*, nor allow third parties to do so. This directly addresses scenarios like Meta combining WhatsApp and Facebook data, or Google consolidating user data across its numerous services, *unless valid user consent is in place*. Importantly, the DCB here explicitly ties the notion of consent to the definition in the DPDPA for end users, creating a bridge between the two laws. Finally, Section 12(3) mandates that SSDEs must allow users (both end users and business users) to easily port their data to other services in a specified format. This effectively introduces a portability requirement that was missing in the DPDPA.

The DCB thus squarely recognizes data portability, interoperability, and prevention of data abuse as pro-competitive measures. The obligations on SSDEs are to be overseen and enforced by the CCI (the DCB envisages CCI as the implementing agency, augmented possibly by a specialized Digital Markets Unit). Non-compliance could attract penalties or remedial orders. The DCB, if enacted, will operate alongside the Competition Act, 2002 – focusing on preventive regulation of the biggest players, whereas the Competition Act continues to apply to all and is enforced *ex post.*

From a privacy perspective, it's notable that the DCB uses the language of "consent" identical to the DPDPA and requires it for cross-use of personal data. This is a clear instance of intended complementarity: the competition law tool (DCB) defers to the standard set by the privacy law (DPDPA) for what is acceptable data sharing. In practical effect, Section 12(2) DCB means a gatekeeper cannot circumvent the DPDPA's consent requirement when leveraging data – and even with consent, the CCI may keep a close watch to ensure that consent is truly voluntary and not extorted by dominance.

However, potential tensions and gaps between these frameworks can arise. One immediate observation is that while DCB Section 12(3) compels SSDEs to enable data portability, the actual transfer of personal data from one service to another still hinges on user approval and perhaps cooperation between services. The DPDPA would require the user to initiate or consent to such porting. If users are apathetic or if the process is cumbersome, the goal of portability (to lower switching costs and foster competition) may not fully materialize. Another subtle tension is that the DPDPA, being consent-centric, might legitimize certain data practices that the DCB forbids in the interest of fairness. For example, a business user on a large platform might *consent* (perhaps under pressure) to the platform's use of its non-public data – but the DCB would still deem it illegal for the platform to exploit that data against the business user. In such a case, competition law is stricter: even consent from the counterparty doesn't permit the conduct, reflecting a judgment that the power imbalance and market distortion are too great. Conversely, there could be situations where competition law might desire data sharing to increase competition (like mandating interoperability or data access for rivals), but privacy law would rightfully object unless each user affected consents. For instance, forcing a dominant social network to share certain user data with competing apps might help competition, but doing so without user consent would violate privacy rights, thus any such remedy must be predicated on giving users choice.

Overall, the Indian legislative and regulatory landscape is moving towards a concurrent application of privacy and competition norms to digital platforms. The DPDPA provides individual-centric rules for data handling, and the Competition Act/DCB provide market-centric rules to prevent anti-competitive exploitation of data. The next section will delve into how these interfaces have played out in concrete cases, and how similar issues have been handled in the European Union, thereby illuminating the practical challenges and solutions in managing the overlap between these frameworks.

2.8: Comparative Jurisprudence: European Union and the German Meta Case

The European Union's experience with big tech regulation offers a valuable comparative perspective, as the EU has been at the forefront of both data protection law (with the General Data Protection Regulation, GDPR) and competition enforcement against digital giants under Articles 101 and 102 of the Treaty on the Functioning of the EU (TFEU). In recent years, the EU has also adopted ex ante rules through the Digital Markets Act (DMA) – analogous in many ways to India's proposed DCB – to curb the power of "gatekeeper" platforms.

Under Article 102 TFEU, which is conceptually similar to Section 4 of the Indian Act, the EU has traditionally pursued cases of abuse of dominance involving predatory pricing, exclusive dealing, tying, refusal to deal, etc. Historically, privacy or personal data considerations did not feature explicitly in abuse cases. Dominant firms exploiting consumers typically meant excessive pricing or other tangible harms. However, as early as the mid-2010s, EU competition authorities began to acknowledge privacy in their analyses. Notably, in some merger control decisions, the European Commission considered the impact of data concentration on privacy as a parameter of quality. For example, in the 2014 *Facebook/WhatsApp* merger review[18], the Commission noted that privacy policies could be a dimension of non-price competition between services, though it ultimately cleared the merger, partly because WhatsApp had promised not to share data with Facebook (a promise later broken). Likewise, in the *Microsoft/LinkedIn* merger (2016)[19], the Commission examined whether combining LinkedIn's data with Microsoft's could give an unmatchable advantage – and it extracted commitments regarding data usage. These instances signalled that the EU recognized privacy as an aspect of competition

[18] **European Commission. (2017, May 18).** *Case M.8228 – Facebook/WhatsApp: Commission decision pursuant to Article 14(1) of Regulation (EC) No 139/2004* (Official Journal C 243, 25.7.2017). https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf

[19] **European Commission. (2016, December 6).** *Mergers: Commission approves Microsoft's acquisition of LinkedIn* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_16_4284

when it mattered to consumers' choices[20]. Commission officials publicly stated that a loss of privacy can be seen as loss of quality, and thus if a merger or conduct reduces privacy, it could be viewed as harming consumers in competition terms.

The paradigm-shifting case was the Bundeskartellamt (German Federal Cartel Office) vs. Facebook[21]. In 2019, the Bundeskartellamt found that Facebook had abused its dominance in the German social networking market by imposing unfair terms on users regarding data collection. Specifically, Facebook's terms allowed it to collect user data not just from the Facebook platform, but also by tracking users on third-party websites and apps (via Facebook's plugins, like buttons, etc.) and merging this data with the users' Facebook profiles – all without their consent beyond agreeing to the general terms. The FCO held this to be an exploitative abuse: users were practically forced to agree to an extensive invasion of privacy to use the dominant social network, which constituted an "exploitative business condition" under German competition law (analogous to unfair condition). Furthermore, the FCO also reasoned that this behavior had *exclusionary effects*: by amassing such comprehensive data, Facebook entrenched its market position, creating barriers for competitors who, respecting privacy or lacking such cross-site tracking, could not compete on equal footing[22]. The FCO's theory thus tightly intertwined privacy and competition harms.

Facebook challenged this decision, leading to a complex appellate saga. The Düsseldorf Higher Regional Court initially suspended the FCO's order, questioning whether competition law could address GDPR violations. However, in 2020 the German Federal Supreme Court (BGH) provisionally sided with the FCO, reinstating the order. Eventually, questions were referred to the CJEU for a preliminary ruling, resulting in the CJEU's judgment in Case C-252/21 (Meta Platforms vs Bundeskartellamt) delivered in July 2023[23].

The CJEU's judgment (2023) unequivocally held that a competition authority *can consider* infringements of GDPR (privacy law) in the course of assessing abuse of dominance[24]. It stated that while a competition authority cannot declare a GDPR violation *abstractly* (that's for data protection authorities), it can analyze whether the dominant firm's conduct complies with data protection rules as a preliminary question when determining if the conduct is an abuse. If the conduct is found to breach GDPR, that can be evidence of an unfair or exploitative practice. Importantly, the Court confirmed that a breach of privacy rights can constitute an abuse of dominance in itself (if it meets the exploitative abuse criteria). The judgment also noted that even if the data processing is not "inherently illegal" under GDPR, competition enforcers may still take into account privacy restrictions or the lack thereof in assessing competitive effects. In essence, the CJEU blessed the approach that privacy harm and competition harm can go hand in hand and that regulators should not ignore regulatory context. It emphasized that this does not deputize competition authorities as data protection enforcers beyond their remit, but rather allows them to incorporate those considerations to fully gauge market reality[25].

---

[20] **Gorecka, A. (2024).** *On the interplay between competition law and privacy: The impact of Meta Platforms case*. European Competition Journal. University of Strathclyde. https://pure.strath.ac.uk/ws/portalfiles/portal/250673473/Gorecka-ECJ-2024-On-the-interplay-between-competition-law-and-privacy.pdf

[21] **Bundeskartellamt. (2019, February 7).** *Bundeskartellamt prohibits Facebook from combining user data from different sources* [Press release]. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

[22] **Organisation for Economic Co-operation and Development. (2024).** *The intersection between competition and data privacy* (OECD Competition Committee Report). https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6/0dd065a3-en.pdf

[23] **Court of Justice of the European Union. (2023, July 4).** *Case C-252/21: Meta Platforms Inc. and others v. Bundeskartellamt* (ECLI:EU:C:2023:537). https://curia.europa.eu/juris/document/document.jsf?docid=275125&doclang=EN

[24] *Ibid*

[25] **Gorecka, A. (2024).** *On the interplay between competition law and privacy: The impact of Meta Platforms case*. European Competition Journal. University of Strathclyde. https://pure.strath.ac.uk/ws/portalfiles/portal/250673473/Gorecka-ECJ-2024-On-the-interplay-between-competition-law-and-privacy.pdf

From a practical standpoint, the result of the German case is that Meta (Facebook) is required to change how it collects and combines data in Germany – effectively giving users the choice to prevent combining of data from Instagram, WhatsApp, third-party sites, etc., with their Facebook profiles unless they consent. This aligns with GDPR's consent requirements and also attempts to restore a form of competition on privacy: if users value privacy, Facebook should not be able to rope them into data sharing by default purely due to its dominance.

The German case has been closely watched worldwide and is clearly analogous to the CCI's WhatsApp/Meta case – both involve a dominant platform linking data across services in a way that users cannot refuse without leaving the service. The German approach treated it as exploitative abuse; the CCI case did similarly (plus added exclusionary abuse findings). The convergence of outcomes (requiring separation of data unless consented) suggests a global regulatory trend of using competition law to buttress privacy. Far from being an anomaly, the German Facebook case is likely a template for future cases where data and dominance intersect.

Turning to the **Digital Markets Act (DMA)**[26], which came into force in 2022 and became applicable in 2023 in the EU: this new regulation imposes a series of ex ante obligations on designated "gatekeepers", large online platforms that serve as important gateways (currently companies like Google, Apple, Meta, Amazon, Microsoft have been designated). The DMA's obligations explicitly address many data-related practices, reflecting lessons from past competition cases and aiming to pre-empt future harm. Two provisions are especially relevant:

- **DMA Article 5(2)**: It prohibits a gatekeeper from merging private data gathered from its core platform facilities with private data from any other facility of the gatekeeper or with data from third-party services, *unless* the operator has been presented with a detailed option (consent) and has given permission in the sense of GDPR. In effect, a gatekeeper (say Google) cannot automatically pool a user's data from various sources (Gmail, YouTube, Android, etc.) to build a super-profile unless the user *opts-in*. This directly targets the kind of cross-platform data leveraging that both the German and Indian cases dealt with. It ensures that even if GDPR might theoretically allow some combining under certain legal bases, the competition rule (DMA) forbids it unless there's clear consent – and likely regulators will interpret that strictly (not a forced bundle but a real choice). The DCB Section 12(2) as noted is aligned with this approach, which is no coincidence given global regulatory dialogues.

- **DMA Article 6(9)**: It requires gatekeepers to enable data portability for their users, specifically, to provide tools for end users to port their information given by the operator or which is generated through their activity) to other services, *continuously and in real-time* if technically feasible. This goes beyond the one-off portability right in GDPR by ensuring ongoing access. The aim is to reduce lock-in: for example, an SME using a gatekeeper's platform should be able to easily export its performance data, or a social media user should be able to transfer their content to a rival platform. Similarly, Article 6(10) obliges gatekeepers to give access to business users to the data they generate (for instance, an app developer should get analytics from the app store). These provisions, while not framed as privacy rules, significantly empower users and third parties and mitigate the data advantage of the gatekeeper. India's DCB Section 12(3) on portability echoes the spirit of DMA Art 6(9).

Other DMA provisions indirectly relate to data: e.g., requiring openness of app stores (preventing forced use of one store or payment system, which has data implications for who sees transaction data), requiring interoperability of messaging services (so a dominant messenger must allow smaller ones to interconnect, an interesting case where for competition, some sharing of data/content is mandated, raising privacy concerns

[26] **European Union. (2022, September 12).** *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Regulations (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. *Official Journal of the European Union*, L 265, 1–66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

which the DMA addresses by limiting to basic text initially and requiring compliance with privacy laws by the interconnecting firms).

One can observe a pattern: the EU is implementing a dual strategy, using case-by-case competition law (as given in the Facebook matter) to push the envelope in addressing data-related abuses, and simultaneously codifying known problematic conducts in the DMA to impose clear ex ante prohibitions and obligations. The DMA essentially means that some practices that took a decade of legal battles to condemn (like self-preferencing or data combining) are now straight-up illegal for gatekeepers. This is to ensure faster intervention and greater deterrence.

In terms of institutional cooperation, the EU is also taking steps. The European Data Protection Board (EDPB) and the European Competition Network (ECN) have engaged in dialogues about consistent approaches. The OECD paper noted that under EU law, there is a *duty of sincere cooperation* which implies that the competition authorities should consult with the authorities which safeguards the data, when their cases impinge on personal data issues. In practice, when the French Competition Authority examined Apple's App Tracking Transparency (ATT) changes, it sought input from the French privacy regulator (CNIL) on whether Apple was held to the same standards as others, eventually deciding not to intervene because Apple's move, though possibly disadvantaging ad-tech rivals, was deemed privacy-driven and applied uniformly (so not an antitrust abuse but a pro-privacy measure). This underscores that regulators must sometimes balance privacy and competition: in Apple's case, privacy rationale was strong enough that competition enforcers chose to step back (recognizing that protecting privacy can justify restrictions that incidentally hurt some competitors, provided it's not a pretext).

The EU's approach thus far suggests that privacy and competition can be largely complementary, but careful analysis is needed to ensure they don't conflict. For instance, if a dominant firm invokes privacy compliance as a defence for a practice that hinders competition (like refusing to share certain data with rivals citing GDPR), authorities will examine if that compliance is genuinely required or if it's being gold-plated to exclude competitors[27]. Conversely, when imposing a competition remedy that involves data (like mandating interoperability), they will factor in GDPR requirements (e.g., obtaining user consent, data minimization).

In conclusion, the European jurisprudence (especially the German Facebook case and the DMA) reinforces the notion that data practices of dominant firms are a legitimate subject of competition law scrutiny. The EU experience validates some of the CCI's pioneering efforts in the WhatsApp case, while the DMA offers a template for legislative measures like India's DCB. For India, EU's journey offers both inspiration (on integrating privacy values into competition enforcement) and caution (on the need for cooperation between regulators and clear legal standards to avoid business uncertainty). With this backdrop, we now turn to the analysis of the Indian cases themselves, which illustrate how the interface of privacy and competition is playing out in practice domestically.

Chapter 3: Case Law Analysis: CCI's Recent Orders in Digital Markets

This section examines three significant CCI decisions that illuminate the interaction between data privacy and competition concerns in India: (1) Google Android (CCI Order dated 20.10.2022, Case No. 39 of 2018); (2) Google Play Billing (CCI Order dated 25.10.2022, Case Nos. 07 of 2020, 14 & 35 of 2021); and (3) WhatsApp/Meta (CCI Order dated 18.11.2024, Suo Motu Case No. 01 of 2021). While all three involve alleged abuses by dominant firms in the digital economy, the first two primarily address traditional competition issues with implicit data dimensions, and the third explicitly merges privacy and competition issues. Together, they illustrate the CCI's evolving approach and set precedents for the interface of the DPDPA and competition law.

[27] **Organisation for Economic Co-operation and Development. (2024).** *The intersection between competition and data privacy* (OECD Competition Committee Report). https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6/0dd065a3-en.pdf

(1) Google Android Case (2022) – Tying, Exclusivity, and the Android Ecosystem[28]

Background: This case concerned Google's conduct regarding the Android mobile operating system and associated Google services. Android (the open-source OS owned by Google) is used by the vast majority of smartphone manufacturers (OEMs) worldwide including in India, under licenses from Google. The CCI's investigation (initiated on information filed by complainants) focused on a series of agreements Google imposed on OEMs and app developers: notably the Mobile Application Distribution Agreement (MADA), the Anti-Fragmentation Agreement (AFA)/Android Compatibility Commitment (ACC), and certain share of revenue contracts. These contractual restrictions allegedly helped Google cement the dominance of its own apps (Google Search, Chrome browser, YouTube, etc.) on Android devices and excluded competitors.

Key Findings: After a detailed inquiry, the CCI was able to find Google dominating several relevant marketplaces: licensable mobile OS (Android) in India, app stores for Android (Google Play Store), online general search, non-OS specific mobile web browsers, and online video hosting platforms – reflecting the breadth of Google's ecosystem. The Commission held that Google had abused this dominance in multiple ways:

- **Tying/Imposition of Unfair Conditions**: Google's MADA required OEMs who wanted critical Google apps (especially the Play Store) to pre-install the entire suite of Google Mobile Services (GMS) apps (a bundle including Search, Chrome, YouTube, Gmail, etc.) on all devices, with prime placement (home screen). OEMs could not uninstall these apps. The CCI deemed this a forced tying arrangement that imposed an unfair condition on device makers, violating Section 4(2)(a)(i) and also amounting to a supplementary obligation unrelated to the provision of the OS, violating Section 4(2)(d). In effect, if an OEM wanted any must-have Google service, they had to take the whole package – foreclosing rivals from being preset on the device.

- **Exclusive Dealing/Market Access Denial**: By making Google Search the default search engine on Android (through Chrome and a search widget) via these agreements, Google perpetuated its dominant position in search and denied market access to competing search apps. This was found to contravene Section 4(2)(c). Similarly, tying Chrome ensured Google entrenched itself in browsers, and tying YouTube helped it in online video – the CCI saw these as instances of leveraging dominance in the app store market (Google Play) to enter/protect positions in other markets (browser, video), violating Section 4(2)(e).

- **Restriction of Technical Development (Forking)**: The AFA/ACC prevented OEMs from selling devices running any Android forks (i.e., modified Android versions not approved by Google). In practice, this meant no fork (like Amazon's Fire OS) could gain traction via mainstream OEMs, reinforcing Google's control. The CCI held that this limited technical development to the prejudice of consumers – alternative versions of Android (which could potentially be more privacy-friendly or have different features) were foreclosed. This was deemed a violation of Section 4(2)(b)(ii) (limiting technical development).

In sum, the CCI concluded that Google leveraged Android's ubiquity to entrench its dominance across various complementary services, using contractual restrictions and default-setting to disadvantage competitors. Although the case was argued on classic competition harms (foreclosure of competition, denial of market access, tying etc.), the underlying strategy of Google had a clear data dimension: ensuring users remained within Google's ecosystem (Search, Chrome, YouTube, etc.) meant Google could continually harvest user data across these services, strengthening its advertising business. By locking OEMs and therefore consumers into

[28] **Competition Commission of India. (2022, October 20).** *In Re: Alleged abuse of dominance by Google in the Android mobile device ecosystem* (Case No. 39 of 2018). https://cci.gov.in/antitrust/orders/details/1070/0

Google's services, Google not only gained more search queries and video views (direct competitive wins) but also more user data feeding into its algorithms. The CCI's order implicitly recognizes this – e.g., noting that these practices helped maintain Google's hegemony in search ads (a data-driven market). The case demonstrates how dominance in a data-rich market (mobile OS/app store) can be leveraged to consolidate data and users in adjacent markets. The CCI didn't explicitly discuss user privacy here, but it did consider consumer harm in terms of reduced choices and innovation (no alternative app ecosystems or search engines).

Remedies: Penalty imposed through CCI of ₹1,337.76 crore on Google and issued wide-ranging cease-and-desist orders. Remedies included: Google shall not force bundling of apps (OEMs must be allowed to choose which Google apps to pre-install); Google must allow uninstalling of pre-loaded apps by users; no exclusivity for search (users should be free to choose default search); no anti-fork restrictions (OEMs can use forked Android); and allowing hosting of third-party app stores on Play Store, among others. These remedies aim to increase competition and consumer choice, which could indirectly enhance privacy options (for instance, if a forked Android with better privacy came to market, or if users could more easily use a privacy-oriented search engine). Google, notably, argued that some restrictions (like the anti-fork rule) were to prevent security and privacy risks from unvetted Android versions – a justification based on user data protection. The CCI, however, was not swayed, finding the restrictions disproportionate and anti-competitive.

The Android case aligns with global antitrust efforts (the EU had fined Google for similar conduct in 2018). It set a precedent in India by highlighting that control of an ecosystem and user data flow can be used anti-competitively. Post-order, Google was required to implement changes in India (e.g., allowing rival app stores and choice screens for default apps), showcasing a scenario where competition enforcement directly opened up avenues for consumer choice, including potentially choices about data/privacy (e.g., choosing a different browser or search engine that might offer better privacy).

(2) Google Play Billing Case (2022) – Anti-steering and Exploitation in the App Economy[29]

Background: Just days after the Android order, the CCI delivered another blow to Google regarding its Play Store billing policies. This case focused on Google's requirement that app developers selling digital goods or services within their apps (distributed via Google Play Store) must use Google's own payment system which is in the app itself (Google Play Billing) and pay a hefty commission (15-30%) on transactions. Furthermore, Google's policies disallowed apps from informing users about alternative payment methods (like an external web link for payment), a classic anti-steering provision. Complaints were filed by startups and developers in India were alleged that it was an abuse of Google's dominance in the Android app store market.

Key Findings: The CCI found Google to be dominant in the market for app stores for Android (as in the Android case). It then held that Google's mandatory use of its billing system for app purchases and in-app purchases was an obligation of biased and discriminatory conditions on app developers, and also an instance of leveraging dominance in the app store market to harm competition in the market for payment processing services. By forcing all in-app revenue to flow through Google's system (with its commission), Google was effectively denying market access to competing payment processors and shielding its own service from competition, violating Sections 4(2)(a), 4(2)(c), and 4(2)(e). The CCI noted that sale of in-app digital goods is crucial for developers to monetize their work and Google's policy elevated its own interests at the expense of developers and alternate payment platforms[30].

[29] **Competition Commission of India. (2022, October 25).** *In Re: Alleged abuse of dominance by Google in relation to its Play Store policies* (Case Nos. 07 of 2020, 14 of 2021, and 35 of 2021).
https://www.cci.gov.in/images/antitrustorder/en/order1666696935.pdf

[30] **Reuters. (2022, October 25).** *India fines Google $113 million in second antitrust penalty this month.*
https://www.reuters.com/technology/india-fines-google-113-million-second-antitrust-penalty-this-month-2022-10-25/

This conduct had both exploitative and exclusionary facets: exploitative, because app developers had to bear high fees (which could be passed on to consumers or result in reduced output), and exclusionary, because it prevented other payment service providers (who might offer lower fees or innovative payment models) from competing. The CCI specifically called out the anti-steering provision – Google even prohibited language in apps that would tell users about cheaper payment options – as aggravating the harm[31]. Consumers, therefore, often had no idea that say, on a streaming app, they could subscribe via the website at a lower price; they were funnelled into the higher Google Play price, part of which was Google's commission.

While privacy per se was not at issue, data played a role: payment data is valuable, and by monopolizing in-app payments, Google not only earned revenue but also gained insights into user transactions. Competing payment providers (like domestic wallets or UPI-based solutions) were locked out from those transactions on Android apps, which also stymied the development of competing transaction-data repositories that could challenge Google's data trove. Additionally, from a user perspective, being forced to use Google's payment system meant they had to share their financial details with Google rather than perhaps a provider of their choice – a subtle privacy aspect (choice of who handles one's financial data) embedded in a competition issue. The Business Standard later reported the CCI even asked Google to clarify its data sharing policies in Play Billing, suspecting that Google might be using payment data to its advantage in other domains [32](e.g., improving ad targeting). This underscores the overlap: the way a dominant firm restricts data flows (like prohibiting outside payment options) can be both an antitrust problem and a data control strategy.

Outcome: Penalty imposed through CCI of ₹936.44 crore on Google and issued corrective orders: Google was directed to allow app developers to use third-party billing/payment services for in-app transactions; it must not discriminate against apps based on the payment system used; and it shall not restrict developers from communicating with users to educate them about alternate purchasing methods. Essentially, Google must remove the "walled garden" around Android in-app payments. This remedy has pro-competitive and pro-consumer effects – likely leading to lower prices or better offers for app purchases (since developers can avoid or negotiate lower commissions outside), and it also gives users a choice possibly to use payment methods that they trust more or that offer them better privacy (for instance, some users might prefer paying directly via a credit card or a secure wallet rather than through Google).

The Play Billing case is a textbook example of how competition enforcement can empower market participants and indirectly benefit user autonomy. By breaking Google's stranglehold on the app monetization channel, it opens up the space for innovation in payments, including perhaps privacy-enhancing payment tech or local solutions attuned to user needs (like India's UPI). It aligns with DCB's proposed Section 14 on anti-steering and Section 12(1) on not exploiting business user data. If the DCB were in force, Google's behaviour would likely violate multiple provisions (self-preferencing its payment system, non-public transaction data usage, etc.), obviating the need for such an extensive investigation.

(3) WhatsApp/Meta Case (2024) – Privacy Policy Changes as Abuse of Dominance[33]

Background: This case encapsulates the direct interface between data privacy and competition. In January 2021, WhatsApp (owned by Facebook, now Meta) announced an update to its Terms of Service and Privacy Policy. The core change was that WhatsApp users *would henceforth be required to accept* the sharing of certain personal data with Meta and its other products (like Facebook and Instagram) for various purposes including personalized advertising. Under the previous (2016) policy, users had a one-time ability to opt-out of such data

[31] *Ibid*

[32] **Business Standard. (2023, May 12).** *CCI asks Google to share policies on data sharing in app billing*. https://www.business-standard.com/companies/news/cci-asks-google-to-share-policies-on-data-sharing-in-app-billing-123051201015_1.html

[33] **Competition Commission of India. (2024, November 18).** *In Re: Updated Terms of Service and Privacy Policy for WhatsApp users – Suo Motu Case No. 01 of 2021*. https://www.cci.gov.in/images/antitrustorder/en/order1732001619.pdf

sharing. The 2021 update removed that choice – it was presented as a take-it-or-leave-it mandate: if users did not accept the new terms by a deadline, their WhatsApp functionality would eventually be limited and then cut off. This triggered worldwide concern (several countries' regulators stepped in; many users migrated to alternatives like Signal or Telegram in protest). In India, aside from challenges in courts on privacy grounds, the CCI *suo motu* took cognizance of the matter in March 2021, suspecting that the conduct might amount to abuse of dominance.

WhatsApp is the overwhelmingly dominant messaging app in India (with over 500 million users). The CCI's prima facie order in 2021 noted that the "take it or leave it" nature of the policy, and the extensive data sharing envisioned, merited investigation under Section 4. Notably, even as Meta argued that privacy is outside CCI's jurisdiction and is being examined by the courts and the then-pending Personal Data Protection Bill, the CCI insisted it could examine whether WhatsApp's conduct, in the garb of a policy update, was anticompetitive[34].

Findings (Order of Nov 2024): After investigation, the CCI's final order in November 2024 held that WhatsApp (and Meta) had abused its dominant position in the market for OTT messaging apps through the 2021 privacy policy update. The abuse findings were multi-pronged[35]:

- **Exploitative abuse – Unfair Terms**: The CCI concluded that the mandatory nature of the data sharing policy constituted an imposition of unfair conditions on users, violating Section 4(2)(a)(i). Users were essentially told that to continue using a service that had become almost indispensable for communication, they must agree to give WhatsApp and Meta access to personal data (including metadata, contacts, device information, etc.) which could be used for purposes beyond WhatsApp's core messaging function. Given WhatsApp's dominance (due to strong network effects and lack of comparable alternatives at scale), users had no effective bargaining power – their "consent" to the new terms was not freely given but coerced by the threat of service loss. This was exacerbated by the fact that many users had initially chosen WhatsApp for its promise of privacy (WhatsApp famously had end-to-end encryption and a reputation for not mining user data), creating a "legitimate expectation" of privacy which was now being undermined[36]. The CCI noted that such a "take-it-or-leave-it" policy, without opt-out, undermined users' autonomy and privacy – concerns that, while moral/consumer issues on their face, were folded into the competition analysis by recognizing them as unfair trading conditions by a dominant firm. In essence, the CCI treated the loss of control over personal data as a form of harm imposed on consumers due to lack of competition.

- **Exclusionary abuse – Market foreclosure/Leveraging**: The CCI also found that the forced data sharing across Meta's services had anti-competitive effects on markets such as online advertising. By combining WhatsApp's rich user data (including social graphs, usage patterns, etc.) with Facebook's existing troves, Meta gained an even stronger edge in personalized advertising, a market where it was already a leading player. Competing ad platforms (for example, those run by other firms) or potential new entrants would find it harder to match Meta's targeting capabilities without similar data access. The CCI held that this created an entry barrier for competitors in the online advertising market, amounting to denial of market access in violation of Section 4(2)(c). Moreover, Meta was leveraging WhatsApp's dominance in messaging to protect and expand its position in display advertising, violating

[34] **Luthra and Luthra Law Offices India. (2024, March 5).** *CCI's order in WhatsApp's updated privacy policy case: At the crossroads of data privacy and competition law*. Lexology. https://www.lexology.com/library/detail.aspx?g=1e09ee90-7c95-4f1c-acfc-2c42c2732dd5

[35] **Press Information Bureau. (2024, November 18).** *CCI imposes penalty on Meta for violating provisions of the Competition Act, 2002*. Government of India. https://pib.gov.in/PressReleasePage.aspx?PRID=2074431

[36] **Bal, M. (2024, November 26).** *The CCI's order in the WhatsApp privacy policy case highlights the perils of regulators engaging with experimental antitrust*. Esya Centre. https://www.esyacentre.org/perspectives/2024/11/26/the-ccis-order-in-the-whatsapp-privacy-policy-case-highlights-the-perils-of-regulators-engaging-with-experimental-antitrust

Section 4(2)(e). Essentially, WhatsApp was used as a funnel to gather data to fuel Meta's advertising dominance – a classic leveraging of dominance from one market to another.

It's important to stress how the CCI linked privacy and competition here. The unfairness was inextricably tied to a privacy violation – compulsory consent to data use beyond what is necessary for the messaging service. The competitive harm was tied to privacy as well because that data would be used to bolster Meta's ad business, competition in the advertising market suffered. In the CCI's own words, the 2021 Update "undermines users' autonomy, and constitutes an abuse of Meta's dominant position". This directly mirrors the theory upheld in the German case. The CCI even quantified the network effects and lock-in: users could not simply switch to another app because everyone they know is on WhatsApp, and the cost of losing connectivity was too high. Thus, Meta was exploiting that dependence.

No justifiable defence: WhatsApp/Meta contended that data sharing was meant to integrate services and improve user experience/security. The CCI likely gave these arguments short shrift, especially given the backdrop of India's recognition of privacy as a fundamental right and the pending enactment (by 2024, actual enactment) of the DPDPA. The absence of consumer choice was too stark to ignore.

Remedies: The CCI imposed a penalty of ₹213.14 crore on Meta (approximately USD 25 million)[37]. More significantly, it issued behavioural remedies to address both exploitative and exclusionary aspects. The key directives were:

1. **No sharing of WhatsApp user data with Meta (for advertising) for 5 years**: WhatsApp was ordered *not to share* any user data with other Meta companies or services for advertising purposes for a five-year period. This essentially freezes the status quo and prevents Meta from immediately capitalizing on WhatsApp data to strengthen its ad targeting. After five years, the order notes, the general directions (see point 2 below) would apply if Meta attempted such sharing then.

2. **Transparency and Opt-out for other data sharing**: For data sharing *not related to ads*, the CCI stopped short of a blanket ban but imposed conditions:
    - WhatsApp must clearly explain to users what data is shared with Meta companies and for what purpose, linking each category of data to its purpose. This is a transparency mandate aligned with data protection principles (in fact, closely paralleling what the DPDPA and its draft rules require for consent and notice)[38].

    - Crucially, it stated that sharing of user data for purposes except providing WhatsApp service intend to *not be made a condition* for using WhatsApp[39]. In other words, WhatsApp cannot require users to agree to data sharing with Meta as a prerequisite for service. Users must be given a real choice, if they don't agree to, say, their account information being shared with Facebook for improving Facebook friend suggestions, they should still be allowed to use WhatsApp. This is essentially mandating an opt-out option or a reversal to the 2016 regime of voluntary opt-in. It directly remedies the exploitative aspect by restoring user autonomy.

[37] **Internet Freedom Foundation. (2024, November 23).** *The privacy-antitrust paradox: Analysing the CCI's penalty order against Meta and WhatsApp*. https://internetfreedom.in/the-privacy-antitrust-paradox-analysing-the-ccis-penalty-order-against-meta-and-whatsapp/

[38] **International Association of Privacy Professionals. (2024, February 12).** *Decoding India's draft DPDPA rules for the world*. https://iapp.org/news/a/decoding-india-s-draft-dpdpa-rules-for-the-world

[39] **Reuters. (2024, November 18).** *India's competition regulator imposes $25.4 mln fine on Meta over WhatsApp's 2021 privacy policy*. https://www.reuters.com/technology/indias-competition-regulator-imposes-254-mln-fine-meta-whatsapps-2021-privacy-2024-11-18/

- Additionally, for existing users who already "accepted" the 2021 policy, the CCI directed that all users in India be given the choice and information to configure their data sharing preferences (so the remedy applies to everyone, not just new terms).

These remedies, once implemented, align extremely well with what the DPDPA would require in spirit: granular consent for each purpose, and freedom to refuse non-essential data processing. In effect, the CCI imposed what the DPDPA, if it had been operational earlier, might have achieved – ensuring that data sharing beyond WhatsApp's core functionality is subject to user consent and not tied to service. It is a striking example of competition law stepping in to fill a regulatory gap for consumer protection in absence of an active data protection authority at that time.
The order also requires compliance within specified timelines and likely calls for audits or reports on implementation. Meta has indicated it would appeal (and indeed in early 2025, the NCLAT granted an interim stay on the no-sharing order, pending appeal, but not on the fine, as media reports suggest[40]. The legal battle may continue, but the CCI's stance is clear.

Chapter 4: Interface with DPDPA and DCB:

By November 2024, the DPDPA was enacted (though not fully in force) and the DCB draft released. The CCI order explicitly references that WhatsApp's policy would violate users' privacy expectations and notes the forthcoming law. It effectively acts as a bridge until the DPDPA and its Board can take over on pure privacy violations. One can imagine that once the DPDPA is enforced, a company attempting a similar mandatory data sharing policy could face dual scrutiny: the Data Protection Board could treat it as a breach of consent requirements and fine the company, while the CCI could simultaneously treat it as abuse if the company is dominant. Ideally, such a company would not try in the first place knowing both angles of enforcement exist.

The WhatsApp case also illustrates regulatory overlap: The subject matter – misuse of personal data under unfair terms, was within CCI's purview for competition harm and would also be within the Data Protection Board's for privacy harm. This case thus underscores the importance of coordination. Had the DPDP regime been active, the CCI and DPB might need to coordinate on remedy (to ensure consistency, e.g., both would want WhatsApp to offer opt-out).

From a competition standpoint, this case establishes that consumer harm in the form of privacy intrusion can amount to exploitative abuse in India, setting a strong precedent. It also confirms that the CCI is willing to tackle data dominance leveraged into adjacent markets – an approach consistent with global trends.

In conclusion, these three CCI cases collectively demonstrate how data considerations permeate competition issues in digital markets: whether it's Google leveraging data and defaults to exclude rivals or forcing its payment system (data + money capture), or Meta exploiting user data across services, the theme is that control and use of data by dominant firms can lead to anti-competitive outcomes. The CCI's remedies have aimed to restore competitive conditions and user choice, sometimes effectively enforcing privacy-friendly outcomes (even in the absence of a privacy regulator's direct action). This synergy, however, has occurred in an ad-hoc way. The next section will discuss policy recommendations to streamline and harmonize this interface so that moving forward, India's regulators can tackle such issues efficiently and coherently.

4.1: Conclusion and Policy Recommendations

The analysis above highlights that in the digital economy, privacy and competition law are not isolated silos but intersecting regimes addressing different facets of the same phenomena, the power that comes from

[40] **JURIST. (2024, November 20).** *Meta plans to appeal India's CCI order over WhatsApp privacy policy*. https://www.jurist.org/news/2024/11/meta-plans-to-appeal-indias-cci-order-over-whatsapp-privacy-policy/

personal data. The Indian experience with the DPDPA and competition enforcement, set against the backdrop of EU developments, shows both complementarity and tension in the regulatory landscape. On one hand, privacy laws like the DPDPA empower individuals and can prevent exploitative data practices, which inherently supports fair competition by preventing dominant firms from leveraging data advantage unfairly. On the other hand, competition interventions like those by CCI have stepped in to provide protections (like choice and consent) that advance privacy interests when privacy law was absent or lagging. Yet, overlaps also create risk of duplicate oversight or inconsistent obligations if not carefully managed.

Regulatory Overlap: A user policy such as WhatsApp's 2021 update could trigger action under both laws – the Data Protection Board (for violating consent norms) and the CCI (for abuse of dominance). This raises issues of coordination: to avoid double punishment for the same act on one hand, but also to avoid gaps where each regulator assumes the other will act. Currently, the Competition Act's Section 62 envisions coexistence, and indeed both avenues can be pursued because they address different harms – one to individual rights, one to the competitive process. Going forward, it is crucial that the CCI and the forthcoming Data Protection Board of India establish a framework for collaboration. This could take the form of a formal Memorandum of Understanding between the two agencies to share information and consult on matters that implicate both privacy and competition. For instance, if the DPB investigates a major platform for misuse of personal data and finds patterns suggestive of market power exploitation, it could inform CCI. Conversely, if CCI encounters a case like WhatsApp's, it could consult the DPB for expert input on data protection norms (much as the French competition authority consulted CNIL in Apple ATT case). This cooperation would ensure consistency – so that, for example, the DPB doesn't approve a settlement allowing certain data use that the CCI might later prohibit, or vice versa.

Harmonizing Standards: One policy recommendation is to harmonize key definitions and standards across the laws. The draft DCB already cross-references the DPDPA's definition of consent, which is laudable. Similarly, terms like "personal data" should have the same meaning in both contexts to avoid confusion. If an SSDE under DCB is told to allow data portability, and DPDPA might regulate data transfers, their rules should align (perhaps through joint guidelines). The goal should be that compliance with one does not inadvertently result in violation of the other. For example, if under DCB an SSDE shares data with a rival to satisfy interoperability, that sharing should be recognized as a "legitimate use" under DPDPA (with appropriate user notice) so that the SSDE isn't punished for a pro-competitive data sharing. The regulators could issue joint guidance on how companies can navigate both laws – e.g., how to design consent flows that meet DPDPA requirements and also satisfy DCB obligations of user choice.

Preventing Conflict in Remedies: We saw how Apple's pro-privacy measures raised antitrust questions. In the Indian context, suppose a dominant platform restricts third-party data access citing user privacy (like limiting an API to protect user data). The DPB might applaud it, but a competitor might complain to CCI that it's exclusionary. To handle this, the DPB and CCI should evaluate the *bona fides* of such privacy rationales together. If a restriction is genuinely to comply with DPDPA or protect users, the CCI should give it due weight (the *competition assessment must incorporate privacy context*, as the CJEU noted)[41]. Perhaps an arrangement can be that when such a defence is raised in CCI, it seeks the DPB's view on whether less restrictive means could achieve the privacy goal.

Strengthening Privacy Law to Support Competition: India's DPDPA currently lacks a data portability right. As data portability is a crucial tool to reduce consumer lock-in (as seen in DMA and DCB), the government could consider introducing a right to data portability in the future (through amendments or in the Rules by empowering consent managers to handle portability) to complement the DCB's requirements. Similarly, the DPDPA could incorporate the concept of "no forced consent" more explicitly (the draft rules hint at it but

[41] **Gorecka, A. (2024).** *On the interplay between competition law and privacy: The impact of Meta Platforms case*. European Competition Journal. https://pure.strath.ac.uk/ws/portalfiles/portal/250673473/Gorecka-ECJ-2024-On-the-interplay-between-competition-law-and-privacy.pdf

making it an express right would be powerful). This would ensure that exploitative tying of service to data sharing is *per se* a privacy violation – reducing the burden on CCI to intervene for exploitative cases and leaving CCI to focus on the market exclusion aspects. If users always must have a choice regarding supplementary data uses under privacy law, then a lot of exploitative abuse can be nipped in the bud by the DPB's enforcement (as and when users complain or DPB takes note).

Augmenting Competition Law for Digital Markets: The Draft DCB is a major step. It should be enacted with careful calibration to ensure consistency with international norms (to ease compliance for global companies) and with the DPDPA. Some recommendations for DCB specifically:

- Include provisions that explicitly state compliance with DPDPA is not a defence for non-compliance with DCB, except where absolutely necessary to comply with law (this avoids companies using privacy as a shield in bad faith, while acknowledging genuine legal conflicts – basically what EU law implies with duty of sincere cooperation ()).
- Build in a consultative mechanism: e.g., the DCB could mandate that the CCI, when making regulations or assessing obligations related to data (like defining what constitutes "consent" for business users, or reviewing data portability standards), should consult the Data Protection Board.

- Consider formal joint-action clauses: perhaps allow the DPB to refer a matter to CCI if it believes a privacy issue has a competition angle, and vice versa.

Inter-agency Dialogue and Training: Both competition and data protection regulators will benefit from understanding each other's domain. Capacity-building programs, joint workshops, and staff exchanges between CCI and the DPB (and also with sectoral regulators like the IT Ministry, TRAI, etc.) should be instituted. Privacy regulators need to grasp market structures and how certain data practices affect competition (so they can prioritize cases that have broad market impact), while antitrust officials need to understand technology and privacy implications (to craft remedies that don't inadvertently violate privacy or to spot when a data practice is harmful beyond traditional metrics).

Consumer Awareness and Empowerment: Ultimately, both laws rely on users exercising choice – either by market switching (competition) or by informed consent (privacy). The government and civil society should invest in programs to educate users about their rights under DPDPA (like right to withdraw consent) and options in digital markets. The easier it is for consumers to port data or choose privacy-friendly services, the more competitive pressure incumbents face to respect privacy. For example, promoting the use of interoperable standards and data portability tools can make it viable for new entrants to attract users (knowing users can bring their data along). India's UPI in finance is a great example of interoperability fostering competition; similar thinking could apply to social media or e-commerce (through open networks or data fiduciaries). The DCB could encourage standard-setting for interoperability in messaging, social media, etc., in a privacy-compliant way. This aligns incentives: competition pushes for more data sharing (with consent), privacy law ensures it's user-driven and safe.

Ensuring No Regulatory Void: There will be areas not directly addressed by either law – e.g., misuse of aggregated non-personal data to foreclose competition (which DPDPA doesn't cover as it's non-personal, and competition law could cover under general abuse). The committee on Non-Personal Data recommended sharing of certain community data for public good, which intersects with competition (access to datasets). Policymakers should be alert to emerging issues like AI training datasets monopolies – which might require collaborative regulation (ensuring dominant firms don't exclusively hoard data needed for AI, while respecting privacy by perhaps using anonymized data pools). This could be a frontier where a joint task force of competition, data protection, and IT experts deliberate on policy.

Following EU's Lead Cautiously: India can draw inspiration from EU's DMA implementation and the German case outcomes. At the same time, it should tailor solutions to India's context. For instance, India's market has some unique features (the prevalence of WhatsApp, UPI, etc.). Solutions like account aggregators

and consent managers in India might provide innovative ways to achieve both privacy and competition goals (e.g., a consent manager could serve as a mediator that porting data from one service to another happens with user's logged consent trail). Policy should encourage such intermediaries that empower users and small businesses – effectively acting as pro-competitive data fiduciaries.

Avoiding Excessive Burden on Businesses: A coordinated approach can also help ensure that compliance with privacy law can serve as a mitigating factor in competition law. If a company designs its systems privacy-friendly (data minimization, user control), competition regulators might view that as a positive factor if any complaint arises that such design limited data to others. Conversely, if a company flouts privacy principles to gather more data, that could aggravate its antitrust liability (as seen, non-compliance with GDPR helped prove Facebook's abuse[42]. Thus, aligning incentives: companies that proactively honor privacy (perhaps even beyond legal minimum) should be less at risk of competition sanctions, unless other anti-competitive conduct exists.

Policy Recommendations Summary:

To encapsulate, the Paper recommends:

- **Formal Cooperation Mechanism**: Establish a coordination committee or MoU between CCI and Data Protection Board for information-sharing on cases of mutual interest and developing consistent policy approaches.

- **Joint Guidelines**: Issue joint guidelines on topics like consent and competition, data sharing and anti-competitive agreements, to clarify expectations for dominant digital firms (for instance, guidance that "take-it-or-leave-it" consent for supplementary data is both a privacy violation and an antitrust concern).

- **Amendments/Rules**: Introduce data portability and perhaps a right to object to processing in the DPDPA through rules or amendments, to empower users further (thus indirectly fostering competition by reducing lock-in).

- **Enact DCB with synergy**: Pass the Digital Competition Act ensuring its obligations (especially Section 12 on data) complement the DPDPA – including requiring SSDEs to implement data interoperability in a privacy-compliant way and giving CCI power to penalize violation of those data obligations (with consultation with DPB if needed).

- **Capacity building**: Train regulators on each other's domains; potentially have a DPB expert as a non-voting advisory member in certain CCI digital market cases and vice versa.

- **Monitor and Adjust**: The digital market evolves rapidly. Set up a mechanism (perhaps a joint review committee) to periodically evaluate how the interface of laws is working – for example, two years after DPDPA and DCB are in operation, assess if companies face contradictory demands or if enforcement has been complementary, and adjust via policy or legislative tweaks.

- **Global cooperation**: Engage in international dialogues (through OECD, G20, etc.) on competition and privacy, as these issues are global with multinational tech firms. India can both learn from and contribute to global best practices, ensuring our regulatory overlap solutions are in line with global trends (this helps companies comply seamlessly across jurisdictions).

In conclusion, India stands at the cusp of implementing a robust framework for the digital economy through the DPDPA and potentially the Digital Competition Act. The overlap of privacy and competition is both an

[42] *Ibid*

opportunity and a challenge: an opportunity to provide comprehensive protection to consumers and ensure fair digital markets, but a challenge in orchestrating two different regulatory philosophies. The key is to remember that both ultimately seek to serve consumers, one by protecting their personhood and autonomy, the other by protecting their economic interests and choice. If approached in a harmonized manner, the two can be mutually reinforcing. A dominant firm should not be able to exploit personal data to the detriment of competition, nor should it be able to hide behind competition excuses to violate privacy. With thoughtful regulatory design and cooperation, India can ensure that the digital economy remains both open and trust-worthy, allowing data-driven innovation to thrive without compromising on fundamental rights or competitive fairness.

Chapter 5: Challenges in Harmonizing the Digital Data Protection Act, 2023 and Digital Competition Bill, 2024

While the Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Competition Bill, 2024 represent landmark developments in India's legal framework for digital markets, their simultaneous evolution raises crucial challenges. These two legal regimes are grounded in different philosophies, the DPDPA seeks to uphold individual privacy and autonomy, whereas competition law is aimed at maintaining market fairness, innovation, and consumer welfare. When data becomes both a personal right and an economic asset, the intersection of these regimes creates a space ripe for legal friction, jurisdictional conflict, and enforcement dilemmas.

This chapter explores the key challenges India may face in harmonizing these two frameworks and highlights the potential institutional, doctrinal, and practical tensions that could undermine their effective implementation.

- **Jurisdictional Overlaps and Regulatory Fragmentation**

  One of the most significant challenges arises from the overlapping jurisdiction of the proposed Data Protection Board (DPB) under the DPDPA and the Competition Commission of India (CCI) under the Competition Act.

  1. The DPB is tasked with ensuring that data fiduciaries process personal data in a lawful, fair, and transparent manner, guided by consent and purpose limitation.
  2. The CCI, in contrast, focuses on detecting abuse of dominance, cartelization, and anti-competitive mergers, especially in the context of digital platforms that aggregate user data.

  Let's consider a situation where a tech firm refuses to share user data with a competitor, citing data privacy under the DPDPA. While the DPB might support this refusal on privacy grounds, the CCI could consider it a case of data hoarding or denial of essential facility, thereby stifling competition.

  This jurisdictional ambiguity raises the risk of conflicting decisions, regulatory delay, and forum shopping by digital firms. Without a clear coordination mechanism, enforcement will likely be fragmented and inefficient.

- **Doctrinal Tensions Between Data Privacy and Competition Goals**

  At a more fundamental level, the normative goals of data protection and competition law may conflict in practice:

  The DPDPA is rights-based, concerned with the dignity and autonomy of individuals. It emphasizes data minimization, purpose limitation, and consent-based processing.

  In contrast, the Competition Bill is market-based, focusing on efficiency, consumer welfare, and competitive dynamics.

  This leads to contradictions. For example:

1. **Data Portability:** Promoting user data portability enhances competition by allowing consumers to shift services easily. However, data portability may also risk compromising privacy if consent mechanisms are weak or if sensitive data is inadvertently shared.
2. **Data Sharing Mandates:** The CCI might push for mandatory data sharing with smaller firms or start-ups to level the playing field. But this could clash with the DPDPA, especially if the data in question is personal and the original users have not explicitly consented to such sharing.

Thus, the legal interface needs to balance user rights with market efficiency, a task that is both delicate and complex.

- **Data Ownership and the Absence of a Clear Legal Doctrine**

Another critical issue lies in the uncertainty around data ownership. Indian law, including the DPDPA, does not currently define data ownership clearly. While the DPDPA provides individuals with certain rights over their data, it stops short of declaring data as the property of the individual. This legal ambiguity creates tension when interpreting anti-competitive behaviour related to data access.

1. Big Tech firms often act as de facto owners of vast datasets, arguing that since they have invested in collecting and organizing the data, they have exclusive rights over its use.
2. From a competition perspective, such exclusive control over data may erect barriers to entry and entrench monopolistic dominance, especially in sectors like search, e-commerce, and digital advertising.

Without a statutory doctrine of data ownership, it becomes difficult for either the CCI or the DPB to adjudicate disputes around access to data, data portability, or data sharing obligations. The lack of clarity can lead to regulatory paralysis or overreach.

- **Enforcement Inconsistencies and Capacity Gaps**

Both the DPB and the CCI face capacity constraints in dealing with the technological complexity of digital markets. Data-driven dominance involves complex assessments, such as algorithmic opacity, behavioural profiling, and real-time bidding, that require a multidisciplinary approach, blending law, economics, and technology.

Some challenges here include:

1. **Lack of technical expertise** within both bodies to understand AI/ML systems and how data is used for competitive advantage.
2. **Inconsistent thresholds** for enforcement: While the CCI operates with market share and dominance thresholds, the DPB works with principles like "reasonable expectation of privacy," which are more subjective.
3. **Delayed enforcement**: Given the pace of innovation in digital markets, regulatory interventions must be **timely and anticipatory**, not ex-post and reactive. Unfortunately, both regulators are known for procedural delays.

Without a coordinated, well-equipped enforcement strategy, there's a risk of **regulatory ineffectiveness**, with big firms continuing to exploit loopholes.

- **Conflicting Remedies and Compliance Burdens**

The enforcement remedies under the DPDPA and the Competition Bill can often be mutually inconsistent, placing digital firms in a compliance dilemma. Some hypothetical examples:

1. The DPB may require a company to delete user data for privacy violations, while the CCI may require preservation of the same data as part of an antitrust investigation.
2. The CCI may direct a dominant firm to open up its API or user data to competitors, while the DPDPA may prevent such sharing without explicit user consent.

This duality leads to a regulatory paradox, making compliance costly, legally risky, and commercially uncertain. Startups and SMEs, in particular, may lack the legal and financial resources to navigate these overlapping frameworks, stifling innovation instead of promoting it.

- **Absence of a Unified Regulatory Philosophy**

Perhaps the most overarching challenge is the lack of a unifying policy vision that integrates privacy protection with competition law in digital markets. Currently, India lacks:

1. A joint regulatory sandbox or interface body for coordination.
2. Shared definitions, such as what constitutes "significant harm" or "public interest" in the digital context.
3. A harmonized legislative intent, with both laws Digitaled in isolation, lacking systemic alignment.

This absence means the laws may pull in different directions, protecting privacy at the cost of competition, or sacrificing privacy in the name of economic efficiency.

India must avoid this false dichotomy. What is needed is a coherent legal philosophy that treats privacy and competition not as rival goals, but as mutually reinforcing pillars of a trustworthy and fair digital economy.

- **International Experience and Lessons**

Jurisdictions like the European Union have already faced similar tensions and have attempted to resolve them through:

1. Inter-agency collaboration between competition regulators (like the European Commission) and data protection authorities (like the European Data Protection Board).
2. The Digital Markets Act (DMA), which mandates data-sharing obligations while upholding GDPR principles.
3. Joint guidelines on data portability, access, and gatekeeping behaviour.

India can **adapt and localize** these lessons to suit its regulatory environment, population scale, and market diversity.

5.1 Conflict between Consumer Choice and Data Control: Harmonizing DPDPA and DCB:

The intersection of data governance and competition law often creates tension between two vital objectives: consumer choice and data control. While the Digital Personal Data Protection Act, 2023 (DPDPA) focuses on empowering individuals with control over their personal data, the Digital Competition Bill, 2024 (DCB) aims to preserve competition and consumer choice in digital markets. However, these goals can sometimes conflict, particularly when data-driven dominance impacts user autonomy and market diversity.

- **Nature of the Conflict:**

1. **Consumer Choice under DCB:**

a) The DCB seeks to prevent the abuse of dominance by large digital platforms (e.g., app stores, search engines, marketplaces).
b) It emphasizes open market access, interoperability, and anti-lock-in measures to enhance user choice.
c) Structural remedies such as data portability and restrictions on self-preferencing are proposed to increase alternatives for users and businesses.

2. Data Control under DPDPA:

a) DPDPA grants individuals the right to consent, correct, erase, and restrict the processing of their data.
b) It imposes obligations on data fiduciaries to ensure fairness, purpose limitation, and transparency.
c) Consent mechanisms and purpose-specific data usage often limit data sharing—even when such sharing could enhance competition.

- **Towards Harmonisation: Policy and Legal Strategies:**

- **Co-Regulation and Joint Guidelines:**

a) Establish a regulatory protocol between the **Data Protection Board** and the **Competition Commission of India (CCI)** to issue joint guidelines.
b) Define principles for data sharing that balance competitive fairness with privacy safeguards.

- **Data Sandboxes and Innovation Zones:**

a) Create controlled environments where businesses can test interoperable and portable data use models under joint oversight.
b) Allow temporary regulatory waivers for pilot innovations that promote both user choice and privacy.

- **Unified Consumer Rights Charter:**

a) Digital a comprehensive charter recognizing both competition-related and data protection-related rights.
b) Ensure that user autonomy, access to alternatives, and data dignity are treated as complementary rather than conflicting values.

- **Standardization and Certification:**

a) Develop technical standards for consent flows, portability protocols, and algorithmic transparency.
b) Certify platforms for privacy and competition compliance, fostering trust and accountability.

The tension between consumer choice and data control is a natural byproduct of regulating the complex dynamics of the digital economy. DPDPA and DCB represent two pillars of digital governance, and their effective harmonisation is essential for achieving a balanced, user-centric ecosystem. By fostering regulatory dialogue, adopting co-regulatory approaches, and crafting interoperable legal standards, India can lead the way in creating a resilient and inclusive digital regulatory architecture where user rights and competition thrive together.

Chapter 6: Institutional Collaboration between the CCI and the Data Protection Board in the Context of the DPDPA and DCB:

In the digital economy, where data is a key driver of both personal autonomy and market power, regulatory oversight must evolve to deal with complex, overlapping challenges. The Competition Commission of India (CCI) and the Data Protection Board (DPB), created under two different legal frameworks, are poised to become the two most critical institutions managing India's digital legal landscape.

As data practices increasingly give rise to both privacy violations and anti-competitive conduct, institutional collaboration between CCI and DPB becomes essential. Without a harmonized approach, regulatory actions could become inconsistent, confusing, and counterproductive. Collaboration can ensure that individual rights and market fairness are protected simultaneously, and that digital innovation is not stifled by conflicting mandates.

- **Institutional Roles Under the Two Laws:**

- **Competition Commission of India (CCI) under the Digital Competition Bill, 2024**
    1. Enforces provisions to prevent abuse of dominance, cartels, and anti-competitive agreements.
    2. Introduces new powers to regulate systemically significant digital enterprises (SSDEs).
    3. May require data access or interoperability as a remedy in digital markets.
    4. Can impose ex-ante obligations to prevent potential harm before it occurs.

- **Data Protection Board (DPB) under the DPDPA, 2023**
    1. Oversees compliance with data protection principles like consent, purpose limitation, data minimisation, and security safeguards.
    2. Handles grievances related to breach of personal data or unlawful processing.
    3. May penalise companies for non-consensual data sharing, profiling, or data misuse.
    4. Ensures that user autonomy and digital dignity are upheld.

- **Need for Institutional Collaboration:** The intersection of privacy and competition law is now a functional reality in digital markets. Examples include:
    1. Data Sharing as a Remedy: CCI may order dominant firms to share data with competitors. But DPB might view this as a violation of consent and privacy rights.
    2. Algorithmic Transparency: Both institutions may demand transparency from digital platforms but for different purposes, privacy protection vs anti-competitive scrutiny.
    3. Consent Mechanisms: If consent is bundled or manipulated, DPB may investigate for violation of privacy, while CCI may examine manipulative or exploitative conduct.

4. Platform Lock-in: Practices like data hoarding can violate both DPDPA's data minimisation principle and DCB's concern with exclusionary conduct.

In such cases, isolated action by either authority could lead to contradictory orders, regulatory uncertainty, and increased litigation. Hence, collaboration is not optional, it is critical.

Chapter 7: Sectoral Analysis of the Interface between the Digital Personal Data Protection Act, 2023 and Digital Competition Bill, 2024

The interface between data protection and competition law becomes most visible and impactful when examined through a sector-specific lens. Different sectors of the digital economy, such as e-commerce, social media, fintech, online advertising, and digital platforms, present unique challenges and opportunities when balancing privacy with market competition. This chapter undertakes a sectoral analysis to assess how the Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Competition Bill, 2024 interact in practical contexts. Through this analysis, we identify the synergies, frictions, and potential areas of regulatory reform in real-world digital markets.

- **E-Commerce Platforms: Data-Driven Market Power:**
    1. **Market Dynamics and Data Dependency:** E-commerce platforms such as Amazon, Flipkart, and Reliance Digital operate as "multi-sided markets" where data is central to operations, from personalized recommendations to dynamic pricing. These platforms collect massive volumes of personal and behavioural data, giving them a strategic edge.
    2. **Competition Concerns:** Under the Digital Competition Bill, 2024, concerns arise over:
    3. **Self-preferencing**: Platforms favour their own products in search results, using consumer data insights to manipulate visibility.
    4. **Exclusive partnerships**: Deals that block rival sellers or restrict platform access.
    5. **Predatory pricing**: Enabled by data analytics to target high-value customer segments.

Privacy Implications

Simultaneously, the DPDPA mandates:

1. Consent-based data processing.
2. Purpose limitation and data minimization.
3. Transparency in algorithmic decision-making.

This creates a conflict: algorithms designed to increase engagement or optimize sales may rely on **data profiling**, but this may violate data minimization principles or exceed the scope of consent provided by users.

Interface Tensions

- The CCI may require data-sharing with third-party sellers to ensure fair competition.
- The DPDPA restricts such sharing unless explicit, informed consent is obtained from users.

Thus, regulators must find a middle ground, ensuring that the platform neutrality and privacy obligations are enforced without stifling innovation.

- **Social Media and Content Platforms: Network Effects and Surveillance Capitalism-**
- **Platform Dominance:** Social media platforms like Meta (Facebook, Instagram), Twitter which is now known as "X", and YouTube thrive on network effects, the more users they attract, the more valuable the platform becomes. This leads to data centralization and the creation of digital monopolies.
- **Data as a Barrier to Entry:** These platforms collect:
    - Personal identity data
    - Behavioural and psychographic data
    - Location and device metadata

  The use of this data to micro-target users and advertisers gives incumbents an anti-competitive edge, effectively locking out new entrants who cannot match the data scale.
- **Privacy Dilemmas:**

  Social media firms have faced global criticism for:

  1. Invasive surveillance practices
  2. Inadequate consent frameworks
  3. Opaque algorithms that manipulate behaviour

  The DPDPA addresses some of these issues, but lacks granular rules on algorithmic transparency, which is crucial for competition analysis.
- **Regulatory Interface:**

  The CCI may order data portability to allow new platforms to attract users, but data transfer may involve third-party or sensitive personal data, triggering DPDPA safeguards.
- **Dark patterns** (design tricks that manipulate user choice) may be examined under both laws, as privacy violations (DPDPA) and unfair market practices (Competition Bill).

  Social media thus exemplifies how **surveillance capitalism** creates a **double regulatory concern**, it undermines both privacy and fair competition simultaneously.

- **Fintech Sector: Data Portability and Consumer Empowerment**
- **The Rise of Fintech:** Fintech platforms, including digital wallets, UPI apps, neobanks, and lending platforms, rely heavily on:

  1. Transactional data
  2. Credit history
  3. Device and location data
  4. Social scoring algorithms

  Fintech companies process sensitive personal data (SPD) and are directly impacted by both privacy and competition rules.

- **Competition Benefits of Data Portability:** Data portability, the ability of a user to transfer their data from one service provider to another, is a **pro-competitive tool**. It allows consumers to switch to better services, thereby increasing competition.

  The **Competition Bill promotes** this as a tool to reduce switching costs and combat data-driven dominance.

The **DPDPA allows for data portability** but only under conditions of clear consent and safeguards.

- **Regulatory Clash**

  In cases where:

  1. A fintech firm denies portability citing security or consent concerns
  2. A regulator mandates it to boost competition

  The absence of **clear enforcement protocols** causes confusion and friction. Regulators must align their definitions of "necessary" data transfer and standardize portability protocols to prevent compliance hurdles.

- **<u>Online Advertising Ecosystem: Market Capture Through Data Profiling:</u>**
- **Structure of the Market:** The digital advertising ecosystem is largely dominated by Google and Meta, which control significant portions of:

  1. Ad inventory
  2. Real-time bidding systems
  3. User targeting technologies

  These firms operate on **cross-platform data collection**, tracking users across websites and devices, creating **closed ad ecosystems**.

- **Antitrust Issues:**
  1. **Preferential ad placements** and exclusive data access harm competition.
  2. Walled gardens restrict third-party access to performance metrics and targeting data.
- **Privacy Concerns:** This tracking often occurs **without informed consent**. The DPDPA's emphasis on:
  1. Granular consent
  2. Limited purpose use
  3. User transparency

  This makes many of these practices legally questionable under data protection law.

- **Interface Example: Real-Time Bidding (RTB):**
  1. RTB involves instantaneous data auctions based on user profiles.
  2. The CCI may view RTB as essential for innovation, while the DPB may challenge it for violating user consent and data security.

  This is a prime example of **regulatory duality**, where one law sees a practice as essential to a competitive market, and another sees it as a **privacy risk**.

- **<u>App Stores and Platform Neutrality:</u>**
- **Dominant Gatekeepers:** App marketplaces such as Google Play and Apple App Store act as gatekeepers, dictating terms for app visibility, revenue sharing, and access to device data.
- **Competition Bill Focus:**
  1. Mandates for fair ranking of apps
  2. Restrictions on self-preferencing
  3. Rules for access to analytics data
- **Privacy Law Implications:**
  a. DPDPA regulates how apps collect and process personal data.

b. It raises concerns when default permissions, background data access, and bundled consents are used.

- **Regulatory Intersection:** A smaller app developer may want access to user analytics from the app store. The Competition Bill may support this for level-playing field purposes, while the DPDPA may prevent it due to lack of user consent or potential overreach into sensitive data.

  This creates a scenario where access to data for competitive fairness conflicts with data minimization and consent architecture under privacy law.

- **Sectoral Observations and Emerging Patterns:** Across all these sectors, some common themes emerge:
  - Data is both a competitive advantage and a privacy risk.
  - Market dominance is often built on data asymmetries, which are hard to dismantle without compromising privacy.
  - Both laws seek to empower the user, but through different mechanisms, competition law by enabling market choice, and privacy law by enforcing data autonomy.

  India's regulatory framework needs to ensure that:
  - User empowerment is holistic, not fragmented across laws.
  - Data portability is standardised across platforms.
  - Regulators co-develop compliance toolkits for each major sector.
  - Joint investigations and coordinated remedies are considered for sectors prone to dual violations.

This sectoral analysis reveals that the interplay between the DPDPA and the Digital Competition Bill is not hypothetical, it is already playing out across industries. Each sector presents distinct challenges requiring tailored, sector-specific regulatory strategies. A "one-size-fits-all" approach is neither practical nor desirable. Ultimately, the India's digital regulation must move toward a model of convergence, where privacy and competition objectives are seen as complementary. The goal should be to create a digital market that is trustworthy, fair, and innovative, underpinned by citizen rights and market discipline.

Chapter 8: Conclusion

The **DPDPA** and the **Proposed DCB** are transformative legislative frameworks that aim to address the critical challenges of privacy and competition in India's rapidly expanding digital economy. While each serves distinct objectives i.e., protecting individual data rights and ensuring fair competition, there are significant intersections that demand careful consideration to prevent regulatory conflicts and maximize the synergies between these frameworks. Balancing the DPDPA's consent-driven approach to data protection with the DCB's focus on fostering competition through data sharing and portability is central to achieving their shared goal of a thriving, equitable digital ecosystem.

To create an effective regulatory environment, fostering collaboration between the Competition Commission of India and the Data Protection Board is essential. Joint efforts can clarify ambiguous areas, such as the use of non-public data, data portability, and the interplay between privacy and competition mandates. This

coordination can result in the development of unified protocols and policies that address overlapping concerns, ensuring both consumer rights and market fairness are preserved.

Moreover, these legislations provide an opportunity to enhance consumer trust and confidence in digital markets. By empowering individuals with greater control over their personal data and simultaneously fostering a competitive marketplace that discourages monopolistic practices, the frameworks can promote a transparent and inclusive digital economy. Such an approach also incentivizes innovation by reducing barriers to entry for startups and smaller players, encouraging creativity and the development of new services and technologies.

India's efforts to align its digital regulatory frameworks with global best practices, such as the EU's General Data Protection Regulation (GDPR) and Digital Markets Act (DMA), will not only enhance the credibility of its legislative ecosystem but also enable the country to effectively engage in the global digital economy. By leveraging international insights and adapting them to the unique dynamics of the Indian market, these frameworks can position India as a global leader in digital governance.

Ultimately, the DPDPA and DCB represent a forward-looking approach to managing the dual challenges of privacy and competition in a data-driven era. By harmonizing their objectives, encouraging regulatory collaboration, and fostering a balance between individual rights and market dynamics, India can establish a robust digital framework that supports economic growth, ensures consumer welfare, and solidifies its position as a global digital powerhouse. The intersection of data protection and competition law is increasingly relevant in a digital-first economy. While the DPDPA and Draft Competition Bill signify progress, their successful implementation depends on mutual coordination and a shared vision of consumer welfare. This dissertation underscores the need for regulatory synergy to curb digital monopolies while safeguarding privacy rights, thereby promoting an inclusive, fair, and innovative digital economy in India.

DPDPA seeks to protect personal data and affirm informational privacy as a fundamental right. It establishes a principle-based structure grounded in lawful processing, purpose limitation, consent, and data fiduciary obligations. The Act also introduces a robust institutional mechanism in the form of the Data Protection Board, tasked with ensuring compliance and accountability across data ecosystems.
On the other hand, the DCB proposes a forward-looking competition law regime that addresses emerging challenges posed by platform dominance, digital gatekeeping, and data monopolisation. Through the introduction of Systemically Significant Digital Enterprises (SSDEs), ex-ante obligations, and merger reforms, the DCB empowers the Competition Commission of India (CCI) with expansive preventive and corrective powers to address structural and behavioural issues in digital markets.

Together these legislations offer a dual lens, rights-based and competition-centric, to evaluate and regulate the conduct of digital enterprises. Their synergy is crucial in a digital economy where data is both an asset and a liability, a tool for innovation as well as exclusion. The overlapping concerns over data collection, platform power, user consent, and information asymmetry make institutional collaboration between the CCI and DPB not just desirable but necessary.
This study has also illuminated how these laws align with global regulatory trends, particularly the European Union's GDPR and Digital Markets Act, positioning India as an emerging regulatory hub. However, implementation remains a complex task, demanding:

- Regulatory clarity and proportionality
- Inter-agency coordination
- Adequate capacity building

- Safeguards against overregulation

Crucially, these frameworks must strike a balance—empowering consumers, enabling startups, and containing dominant platforms—while fostering trust in the digital ecosystem. Regulatory convergence and institutional synergy must be accompanied by legal certainty, stakeholder consultation, and continuous adaptability to technological change.

In conclusion, the DPDPA and DCB are not isolated legal instruments but complementary pillars of India's digital governance architecture. Their interface will shape not only the rules of digital engagement but also the trust infrastructure for the 21st-century economy. A harmonised approach, built on cooperation, coherence, and constitutional fidelity, can ensure that India's digital economy grows in a manner that is inclusive, innovative, and rights-respecting.

Bibliography

Government of India. (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Gazette of India. August 11, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

Carnegie Endowment for International Peace. (2023). Understanding India's new data protection law. October 2023 https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

Ernst & Young (EY). (2023). Decoding the Digital Personal Data Protection Act, 2023. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023.

AZB & Partners. (2023). Digital Personal Data Protection Act, 2023: Key highlights. https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/.

Competition Commission of India (CCI). (n.d.). Advocacy booklets. https://www.cci.gov.in/advocacy/publications/advocacy-booklets.

Primus Partners. (n.d.). Digital Personal Data Protection Act, 2023: Overview and implications. https://primuspartners.in/docs/documents/BFZNHCcaNBqLqsfXFw83.pdf.

Lexology. (n.d.). India's Digital Personal Data Protection Act, 2023: Key highlights. https://www.lexology.com/library/detail.aspx?g=5722a078-1839-4ece-aec9-49336ff53b6c.

George Washington University, Competition Lab. (n.d.). Overview of India's Digital Competition Bill, 2024. https://competitionlab.gwu.edu/overview-indias-digital-competition-bill-2024.

The Dialogue. (n.d.). Brief report of the Committee on Digital Competition Law and Draft Digital Competition Bill, 2024. https://thedialogue.co/publication/brief-report-of-the-committee-on-digital-competition-law-and-draft-digital-competition-bill-2024/.

PRS India. (2024). Report of the Committee on Digital Competition Law (CDCL), March 2024. https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf.

Comptroller and Auditor General of India (CAG). (2024). ICISA journal with special coverage on digital governance. https://cag.gov.in/uploads/icisa_virtual_publishing/Journal-with-cover-DG-message-08-10-2024-06704c77f434894-25842653.pdf.

OECD. (2022). 'Summary of discussion of the roundtable on Ex Ante regulation and competition in digital markets'. https://one.oecd.org/document/DAF/COMP/M(2021)2/ANN3/ FINAL/en/pdf.

Ministry of Corporate Affairs. (2019). "Report of competition law review committee", Indian Economic Service. https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf

Lok Sabha, "Anti-competitive practices by big-tech companies". (2022). https://loksabhadocs.nic.in/lsscommittee/Finance/17_Finance_53.pdf

Parliamentary Standing Committee on Finance. (2022). "Anti-competitive practices by big tech companies", PRS Legislative Research. https://prsindia.org/policy/reportsummaries/anti-competitive-practices-by-big-tech-companies

Latham & Watkins LLP. (2023). India's Digital Personal Data Protection Act, 2023 vs. the GDPR: A comparison. https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.

Organisation for Economic Co-operation and Development (OECD). (2024). Regulating competition in the digital economy. https://one.oecd.org/document/DAF/COMP(2024)4/en/pdf.

Global Competition Review. India: Regulators must balance growth and innovation with user protection. https://globalcompetitionreview.com/guide/data-antitrust-guide/first-edition/article/india-regulators-must-balance-growth-and-innovation-user-protection.

Competition Commission of India (CCI). (n.d.). *Order dated 18.11.2024.* https://www.cci.gov.in/antitrust/orders/details/1158/0.

European Commission. (2022, December 20). *Antitrust: Commission accepts commitments by Amazon to address competition concerns.* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777.