International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-11, Issue-3, July-Sep-2024

Research Article

Harmonizing Competition Regulations and Data Privacy Laws in the Era of Artificial Intelligence

Shilpa Khandelwal
Assistant Professor, Modi Law College, Kota, Rajasthan.

Corresponding Author: Shilpa Khandelwal

Abstract: The passing of the Digital Data Protection Act, 2023 ("Act") has been a milestone for user data privacy in India. However, the Act also holds immense importance from an anti-trust perspective. There has been a growing consensus among academicians and regulatory bodies regarding the potential threats posed by 'Data Harvesting' from the perspective of competition law. The Competition Commission of India ("CCI") has already acknowledged this reality. The way user data is processed and utilized by companies is fundamentally changed by artificial intelligence, thereby rendering the traditional approach towards data protection obsolete. This paper contends that addressing anti-competitive data extraction solely through the Competition Act is overly optimistic and conveniently disregards the Law of the Second Best. This paper contends that there exists a significant overlap between privacy concerns and anti-trust concerns, and both cannot be dealt independently. The tendency of policymakers to ignore the scope of integration between the two frameworks is flawed. This paper suggests the need to acknowledge the confluence of the aforementioned areas, thereby attempting to tackle the emergent legal perils of rapid technological advancement through diverse policy instruments. In this context, the author argues for implementing responsible and mandatory data sharing (under the Competition Act) and the segmentation of consent in certain cases (under the Act).
Keywords: Data Privacy, Anti-Competitive Data Collection, Competition Law, Artificial Intelligence, Wolfgang-Zolna Hypothesis

INTRODUCTION

The rapid development of Artificial Intelligence ("**AI**") and data harvesting has created new challenges for regulating digital markets.[1] This article explores the interplay between competition law and data protection law in this context, arguing that these two frameworks are inextricably linked and must be integrated to achieve market efficiency and consumer welfare.

The central theme of this article is anti-competitive data collection, which refers to the use of user data and AI to exploit market dominance and facilitate anti-competitive mergers. The author analyses the lacunas of the jurisdictional model followed in India, considering the *Wolfgang*

[1] 'Antitrust risks and big data' (*Norton Rose Fulbright*, June 2017) <https://www.nortonrosefulbright.com/en-in/knowledge/publications/64c13505/antitrust-risks-and-big-data> accessed 11 August 2024; *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users* (2021) Suo Moto Case No. 01 of 2021.

Zolna hypothesis.[2] Indian law grants sole jurisdiction to the CCI in these matters. This connotes an oversimplistic understanding of digital markets and disregards *the law of the second best*[3]. The paper proposes an alternative twin-fold solution, combining the tools of the Competition Act and the Act to deal with antitrust concerns in digital markets.

This article argues for a responsible and state-enforced system of mandatory data sharing between big tech companies and emerging players in the market as a remedy for anti-competitive data extraction. The paper also suggests introducing a specific provision in the Act mandating obtaining separate consent in cases of potentially harmful mergers, distinct from the general terms of service, drawing inspiration from the EU's Digital Markets Act. The paper concludes by linking AI to the proposed arguments and highlighting the need for harmonizing competition regulations and data privacy laws in the era of artificial intelligence.

THE CONCEPT OF ANTI-COMPETITIVE DATA COLLECTION

In light of the recent technological and regulatory developments, it seems clear that anti-trust, data privacy, and AI frameworks will intertwine to create an inextricable trifecta for market fairness in the years ahead. This idea can be better appreciated by considering how the combination of user data, AI, and machine learning can be utilised to exploit market dominance and facilitate anti-competitive mergers.

Access to an expansive user data pool offers an undeniable competitive edge, enabling big-tech companies to leverage advanced machine- learning tools for comprehensive data analysis, leading to superior product development and increased customer attraction. The phenomenon can be understood as a slightly tweaked version of the well-known *network effect*, i.e., a phenomenon where the value of a product or service increases with the number of users. As the user share of a product grows, breaking into the market becomes increasingly challenging for new players. This dynamic can easily foster a vicious cycle, depending on which side of competition a business finds itself in.

The potential of data as a powerful tool for non-price competition is recognised by the *CCI Telecom Report*,[4] enabling enterprises to gain a competitive edge over their rivals. Furthermore, the CCI's Market Study on E-Commerce[5] emphasizes that network effects from extensive data collection enables companies to compete beyond pricing, leading to a *winner takes all* scenario.
Another aspect of data and AI in antitrust regimes is their role in facilitating mergers and acquisitions ("**M&A**"). According to *Frank Mwiti*,[6] AI powered data processing is transforming the way mergers and acquisitions are conducted. This includes efficient deal origination and sourcing by analysing diverse data sources to identify potential acquisition targets accurately.

---

[2] Wolfgang Kerber and Karsten K Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2022) 54 European Journal of Law and Economics 217–250 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3719098> accessed 28 July 2023.

[3] The second-best theorem, is a concept in welfare economics which states that if not all distortions in an economy can be eliminated, then attempting to correct one distortion may worsen the overall situation rather than improve it.

[4] Competition Commission of India, 'Market Study on the Telecom Sector in India' (*CCI*, 22 January 2021) <https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf> accessed 16 July 2023.

[5] Competition Commission of India, 'Market Study on E-Commerce in India' (*CCI*, 8 January 2020) <cci.gov.in/images/marketstudie/en/market-study-on-e-commerce-in-india-interim observations1652262845.pdf> accessed 17 July 2023.

[6] Managing Partner & Eastern Africa Markets Leader at Earnst & Young.

Then, AI is deployed to automate tasks like document review, ensuring thorough evaluations while saving time, and minimizing errors. Valuation also gets streamlined by analysing financial data and other relevant information. Additionally, risk management systems based on AI can flag the regulatory hurdles in advance, and in some cases, defeat the legislative intent.

Hence, it is important to recognize the interconnection between non- competitive mergers and the abuse of market dominance. The former lays the groundwork for the latter. The *Google/ DoubleClick merger*[7] serves as a notable example where this relationship was acknowledged by the US Federal Trade Commission ("**FTC**"). On 13 April 2007, Google agreed to acquire DoubleClick for $3.1 Billion. However, the deal raised concerns surrounding competition with the FTC. The Commission noted that such mergers can have "*adverse effects on non- price attributes of competition, including the critical aspect of consumer privacy*".[8]

To streamline the discussion, the term *anti-competitive data collection* will be used throughout this article to encompass the various potential anti-competitive implications of large-scale data collection by big tech companies, as outlined in the preceding paragraphs. Since AI has profound capabilities to facilitate the aforementioned, it is crucial to understand how anti-competitive data collection is regulated. As digital markets present an intersection of concerns regarding data privacy and monopolization, it is pertinent to arrive at the appropriate framework that harmonises data protection and competition enforcement.

WHO SHOULD REGULATE ANTI-COMPETITIVE DATA COLLECTION?

In accordance with the economic equilibrium model, under perfect competition, it is commonly posited that unrestricted markets foster desirable distribution of resources, thereby promoting efficiency of the economy. Any departure from the theoretical *free market*, including but not limited to issues related to competition, information, behavioural biases or technological externalities may result in economic inefficiencies, consequently leading to various forms of market failures. Such deviations may be addressed through diverse economic policies and corresponding instruments, such as conducting merger reviews within the ambit of competition policy, enforcing obligatory information regulations under consumer law, or implementing *Pigou taxes* in the sphere of environmental policy.

Moreover, it is beyond doubt that the simultaneous emergence of two or more significant market failure problems in identical markets is a common phenomenon. The *theory of second best* explains that when multiple market imperfections coexist, seemingly counterintuitive consequences can arise. For instance, addressing one market failure, such as a competition problem, might not necessarily lead to increased efficiency if other unresolved market failures, like information problems, persist simultaneously. In this light, it becomes important to establish an optimum *second best* framework that does not result to market imperfections in other areas.

[7] Case No COMP/M.4731 – Google/ DoubleClick, Commission Decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (*European Commission*, 2008) <https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_2068 2_en.pdf> accessed 10 August 2024.

[8] Federal Trade Commission, 'Federal Trade Commission Closes Google/DoubleClick Investigation' (*FTC*, 20 December 2007) <https://www.ftc.gov/news-events/news/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation> accessed 18 July 2024.

Prof. Wolfgang Kerber and *Karsten K. Zolna* in their seminal elucidation of the *German Facebook Case*, have discussed the commonly accepted solution to this conundrum.[9]

In the legal context, data privacy has transcended from being a mere philosophical concept to a highly valuable and tangible asset. If left unregulated, it may give rise *to information and behavioural problems.*[10] This includes lack of transparency surrounding the collection and utilization of personal data, coupled with the use of misleading information and behavioural manipulation (like employing *dark patterns*). Ultimately, this results in consumers being overwhelmed and unable to make rational and well-informed decisions concerning their personal data. Furthermore, this issue adversely affects competition and creates entry barriers, as consumers are unable to compare data-collection practices of different firms. Consequently, the expected positive impact of competition on privacy-friendly products and services remains unfulfilled. Large digital platform firms, such as Google and Facebook, are able to gather substantial amounts of personal data, bolstering their competitive advantages in various markets.[11]

The impact of competition-related market failures on privacy is also significant. Reduced competition, whether due to dominant firms, data- collection cartels, or consumer lock-in effects, restricts consumer choices for services with varying data-collection and privacy protection levels. Lack of choice arising from market power discourages consumers from scrutinizing privacy policies, potentially leading to even more opaque, misleading, and manipulative privacy practices, further aggravating information and behavioural problems and negatively impacting privacy.

The central question addressed by *Wolfgang* & *Zolna* in their analysis is which law between competition law and data law is better suited to address the above-mentioned market failures. Here, the authors were not directly addressing the issue of jurisdiction, but rather were focused on determining the appropriate legal framework for analysing such matters. However, if applying the Competition Act[12] yields better results, it logically follows that the CCI should deal with the issue.

According to the authors, data protection laws fail to effectively control market failures related to market dominance, a concern addressed by competition law. This is because, such frameworks (including the Act[13]) treat all firms equally without distinguishing between different types, resulting in uniform rights and obligations for each, leading to disproportionate compliance costs.[14] Consequently, a data protection law cannot adequately address situations where privacy standards are compromised due to the monopolization of the market by a single firm with a weak privacy policy.[15]

---

[9] Wolfgang Kerber and Karsten K Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2022) 54 European Journal of Law and Economics 217–250 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3719098> accessed 28 July 2024.
[10] ibid
[11] Stanford Digital Economy Lab, 'EU Digital Markets Act' (*Stanford Digital Economy Lab*, 2021) <https://digitaleconomy.stanford.edu/eu-digital-markets-act/> accessed 8 August 2024.
[12] The Competition Act, 2002 (12 of 2003).
[13] The Digital Personal Data Protection Act, 2023 (22 of 2023).
[14] Bar and Bench, 'Key features and issues in the Digital Personal Data Protection Act, 2022' (*Bar and Bench*, 2022) <https://www.barandbench.com/law-firms/view- point/key-features-and-issues-in-the-digital-personal-data-protection-act-2022> accessed 10 August 2024.
[15] ibid.

Conversely, while maintaining free and fair competition in the market, the Competition Act also safeguards privacy standards. This can be done by discouraging practices with adverse effects on privacy directly, caused by practices deemed to be against the competitiveness, such as mergers that exploit customer datasets. By preventing such mergers from going unnoticed, the Competition Act can protect privacy effectively. This stems from competition laws' capacity to interpret all negative effects on privacy as a reduction in consumer welfare since privacy standards also signify service quality. As competition law directly addresses consumer welfare, it is well-equipped to handle such concerns.[16]

Considering the characterization of the two policy tools discussed above, it is evident that the Competition Act exhibits a more comprehensive approach to addressing the intersection of competition and data protection issues compared to the Act.[17] Consequently, within the framework of this hypothesis, it appears reasonable to assign jurisdiction over overlapping market failures to the CCI. The subsequent sections will delve into a more normative analysis of the *Wolfgang-Zolna theory*.

ASCERTAINING THE JURISDICTIONAL MODEL FOLLOWED IN INDIA IN LIGHT OF THE ACT

As formerly ruled by the CCI in regards to the usage of data, an organisation like Facebook possess the *potential to collect and process significant amounts of customer data*.[18] Building further upon this perspective, the *WhatsApp Suo Moto Order* issued by the CCI stated that the competition law must scrutinize about ecosystems that are particularly orchestrated by data, whether *excessive data collection* and the subsequent utilization or sharing of such-collected data have anti- competitive implications that require antitrust scrutiny.[19] Regrettably, Indian Jurisprudence has not witnessed significant progress regarding the issue of excessive data collection in relation to its impact on market competition. Excerpts from Section 10[20] of the Act have been produced below to exemplify this point.

- Section 9 (2)[21]: *A Data Fiduciary shall not undertake such processing of personal data that is likely to cause harm to a child, as may be prescribed.*
- Section 9 (3)[22]: *A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.*

Further, under Section 10(1),[23] "the Central Government has the authority to designate Data Fiduciaries or a class of them as Significant Data Fiduciaries based on various factors, including the volume and sensitivity of personal data processed, risk of harm to the Data Principal, impact on India's sovereignty, risk to electoral democracy, security of the State, public order, and any other relevant considerations." For Significant Data Fiduciaries, an extra burden of compliance is imposed. They are required to appoint a Data Protection Officer based in India, who represents them and handles grievance redressal. They must also engage an Independent Data Auditor to assess their compliance with the Act.[24]

---

[16] ibid.
[17] The Digital Personal Data Protection Act, 2023 (22 of 2023).
[18] "Combination Registration No. C-2020/06/747, <http://164.100.58.95/sites/default/files/Notice_order_document/order-747.pdf> accessed 18 July 2024.
[19] ibid.
[20] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 9.
[21] ibid s 9 (1).
[22] ibid s 9 (2).
[23] ibid s 10 (1).
[24] ibid s 10 (2).

Nonetheless, the problem remains unsolved from the point of view of competition law as there are no mechanisms in place to expressly restrict anti-competitive data collection per se. This absurdity can be explained as a part of the prevailing inclination in Indian Jurisprudence to maintain a clear demarcation between Competition Enforcement and Data Privacy Frameworks, presuming that their objects are extricable. The Competition Law has the sole jurisdiction on matters where there is an overlap between Data Privacy and Antitrust concerns. This indicates strict adherence to the *Wolfgang -Zolna Model* in Indian law and practice.

THE LIMITATIONS OF THE WOLFGANG-ZOLNA HYPOTHESIS

The CCI presented its findings to the *Parliamentary Standing Committee on Finance* in 2022, highlighting numerous investigations into anti-competitive practices by technological giants in the digital space.[25] During the presentation, the CCI informed the Panel about the establishment of a *Digital Markets and Data Unit* and proposed amendments to the Competition Act to effectively address the emerging anti-competitive practices in the digital domain. As a result, the Committee expressed its concern and is planning to engage in discussions with major players like Google, Twitter, Amazon, and others.[26]

The CCI is presently occupied in a proactive endeavour to fortify its regulatory prowess concerning digital markets through the establishment of the said in-house *digital market data unit*.[27] The primary objective of this initiative is to position the CCI as a *force multiplier*, thereby enabling it to effectively confront the multifaceted challenges inherent in the realm of complex technology markets.

This approach from the Parliamentary Committee and the CCI is praiseworthy. However, the author believes that certain amendments to the Act are also necessary, if only to complement the provisions of the Competition Act. When we try to define the jurisdiction of the two regulatory bodies without accounting for the overlap in subject area, conflicts and paradoxes inevitably arise. This argument would be developed properly in the following paragraphs.

As argued by *Kuenzler*, granting sole jurisdiction to the Data Protection Board would require reliance on the objectionable presumption that that consumers are entirely susceptible to manipulation and wholly vulnerable to exploitation. Likewise, it would also be highly objectionable to maintain that all consumers are completely sovereign, acting as rational calculators, who consistently make optimal choices in the market, justifying the assignment of complete jurisdiction to the competition regulator. Both of these extreme conditions would be overly stringent and contentious, making it impractical to base a specific institutional arrangement solely on them.[28]

---

[25] Saurav Kumar, 'Analysing the Joint Parliamentary Committee Report on the Competition Amendment Act, 2022' (*SCC Blog*, 14 January 2023) <https://www.scconline.com/blog/post/2023/01/14/analysing-the-joint-parliamentary-committee-report-on-the-competition-amendment-act-2022/> accessed 9 August 2024.

[26] PTI, 'Parliament Panel to Summon Google, Twitter, Amazon, Other Big Tech Firms to Discuss Their Competitive Conduct' *The Economic Times* (28 April 2022) <https://economictimes.indiatimes.com/tech/tech-bytes/parl-panel-to-summon- google-twitter-amazon-other-big-tech-firms-to-discuss-their-competitive-conduct/articleshow/91154905.cms?from=mdr> accessed 19 July 2024.

[27] Lele Sourabh, 'CCI to Set up In-House Digital MKT Data Unit for Regulating Tech Platforms' *Business Standard* (22 March 2023) <https://www.business- standard.com/article/companies/cci-to-set-up-in-house-digital-mkt-data-unit-for- regulating-tech-platforms-123032200133_1.html> accessed 24 July 2024.

[28] Adrian Kuenzler, 'What Competition Law can do for Data Privacy (and vice versa)' (2022) 47 Computer Law and Security Review 105757

Data privacy regulations frequently enforce compliance obligations on organizations, without discerning between businesses of varying scales, further observed in the Act. Consequently, the costs associated with compliance can be highly disproportionate. Specifically, the costs associated with following the data privacy regulations may erect substantial obstacles for emerging enterprises, promote efficiencies in size, and offer benefits to well-established participants.

For an instance, the General Data Protection Regulation ("**GDPR**") has been estimated to cost close to a million dollars in compliance, acting as a substantial entry barrier.[29] While the Act is a simplified data protection law, and may not lead to similarly enormous costs, it remains probable to enforce considerable costs, unfairly affecting smaller participants.

The Act introduces a uniform requirement for specific, positive, and unambiguous consent (Section 6 (1)),[30] which could potentially lead to imbalanced impacts on less diversified and smaller data trustees in contrast to their larger counterparts. To explain further, let us explore a cost of compliance "n" that remains relatively consistent among companies of size[31] X and 10X. When we assess the influence in terms of cost per size, it becomes clear that n/X has a less advantageous outcome than n/10X, granting a benefit to more sizable enterprises compared to their smaller counterparts. *Campbell* and colleagues additionally contend that opt-in consent (affirmative consent) privileges broader, versatile businesses over niche specialists.[32]

Likewise, the demand for explicit approval as outlined in Section 6(1)[33] might give rise to worries about anticompetitive practices. Privacy rules mandating specific consent on data usage or sharing tend to encourage consolidation. *Picker* suggests that firms may opt for vertical or horizontal integration to bypass sharing requirements.[34]

Furthermore, a high consent threshold may perpetuate advantages for larger firms. *McDonald* and *Craner* propose that due to uncertainties created by data protection laws, consumers may trust their data more with larger firms, giving already established companies easier access to data and facilitating their growth.[35]

<https://www.sciencedirect.com/science/article/pii/S0267364922001005#:~:text=If%20the%20practices%20of%20these,of%20their%20products%20and%20services>.

[29] Anupam Chander et al, 'Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (*World Development Report 2021, Policy Research Working Paper 9594, World Bank Group*, March 2021) <https://documents1.worldbank.org/curated/en/890791616529630648/pdf/Achievin g-Privacy-Costs-of-Compliance-and-Enforcement-of-Data-Protection- Regulation.pdf>; International Association of Privacy Professionals, 'Survey: GDPR Compliance Costing Millions' (*IAPP*, 12 December 2017) <https://iapp.org/news/a/recentsurvey-shows-gdpr-compliance-costing-millions/> accessed 5 August 2024.

[30] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 6 (1).

[31] Size can be roughly equated with the Market Capitalization of the company for the purpose of this analogy.

[32] Priyansh Dixit and Sukaram Sharma, 'Balancing Privacy and Competition: Evaluating the Competitive Effects of India's Data Protection Act' (2023) 44 (2) Statute Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4486830>.

[33] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 6 (1).

[34] Randal C Picker, 'Competition and Privacy in Web 2.0 and the Cloud' (*Chicago John M. Olin Law and Economics Working Paper No. 414*, 17 June 2008) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985>.

[35] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) Journal of Law and Policy for the Information Institute 543 < https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>.

While the *Wolfgang-Zolna* theory's assertion of Competition Law's primacy in addressing anti-competitive data collection might seem intuitively appealing, closer scrutiny reveals its limitations. Several academic works implicitly challenge its conclusions. In this light, we can better examine the merits of the jurisdictional model followed in India.

APPROACHING MANDATORY DATA SHARING THE RIGHT WAY

It now becomes clear that the *Wolfgang-Zolna* hypothesis is flawed insofar as it seeks to unilaterally solve the kerfuffle between the data privacy and antitrust regulatory landscape by conferring sole jurisdiction to the CCI in regards to data driven anti-trust concerns. However, there exists an easy fix which does not require us to re- evaluate the fundamental tenets of the *Wolfgang* hypothesis. Most of the aforementioned problems, including the issue regarding data-sharing and the regressive cost of compliance could be resolved by including a separate requirement limiting the amount of data collection where it might provide an unjust competitive advantage to the data holder, or its parent company.

Trying to ascertain the markets where the competitive value of user data is high is not an entirely novel endeavour. A 2020 study published in Harvard Business Review exemplifies this point.[36] For example, *Mobileye*, a leading provider of Advanced Driver-Assistance Systems ("**ADAS**"), significantly benefits from customer data to improve the accuracy of its systems to 99.99%. On the other hand, some businesses, like smart television manufacturers, have relatively low value added from customer data as it does not significantly influence consumer purchasing decisions. In that market, the primary features consumers look for are screen size, display quality, and durability.[37]

The article also highlights the difference in the rate of diminution of marginal value of data-enabled learning in different markets. Businesses with a slow drop-off in marginal value tend to have strong competitive barriers, whereas those with rapid drop-offs may not gain significant competitive advantage. The example of Mobileye's ADAS shows that even following the attainment of a substantial customer foundation, the incremental worth of gleaning insights from customer information remains significant, resulting in significant competitive advantages and a dominant market position. In contrast, businesses like smart thermostats have a quick drop-off in marginal value as they only need a short period to learn user preferences. In such cases, data- enabled learning does not provide substantial competitive advantage.[38]

Such studies demonstrate that attempts are ongoing to ascertain the kinds of markets where *data extraction* can have significant anti- competitive effects. The problem that props up now is relating to the fact that products, where user data has significant competitive value, are by very definition dependent on large volumes of data to become safely operational. The example of Mobileye mentioned above, for instance, is a company involved in the business of building smart driver assistance software solutions and automated driving systems. Compromising the accuracy of the output of such a product could be devastating and could lead to real life consequences on the field. This risk reasonably deters anyone from prescribing a blanket limit on the quantity of data extraction. Therefore, the intuitive solution does not work.

[36] Andrei Hagiu and Julian Wright, 'When Data Creates Competitive Advantage (And When it Doesn't)' (*Harvard Business Review*, February 2020) <https://hbr.org/2020/01/when-data-creates-competitive-advantage> accessed 6 August 2024.
[37] ibid.
[38] ibid.

The idea of obligatory data sharing is gaining traction as a possible solution. In theory, this method can ensure continued product development whilst also cutting down the entry barrier created by the consolidation of data in the hands of a few big tech-companies. The EU Data Act Proposal, for example, covers different aspects relating to data-sharing, ranging from access to data generated by connected devices (e.g., internet of things (IoT)), mandatory B2G sharing in exceptional circumstances.[39]

The CCI has also prescribed *compulsory data sharing* in the past. In a ruling dated 25 October 2022, the CCI imposed a penalty of 937 crores on Google for exploiting its dominant market position, as stipulated in Section 4 of the Competition Act.[40] The order contains a peculiar remedy that has not garnered adequate attention. The CCI therein required Google to share individual user transaction details with fellow app developers on its play store.[41] The commission argued that such information enabled Google to deliver precise targeted advertisements, thereby conferring a discernible competitive advantage to the tech giant that other app developers could not access.

Although Section 6 of the Act[42] emphasizes the necessity of specific consent, thereby restricting data fiduciaries from freely sharing data with others without consumer authorization, it also includes considerably broad exceptions. Section 7 introduces the concept of *deemed consent,* implying that consent will be presumed to have been given, if required, for public order, compliance with existing laws, or judicial orders.[43] Notably, the Act goes even further, providing a sweeping exception for *public interest*, making the scope of excluded categories much broader than the European GDPR.

Hence, although obligatory data-sharing might initially seem disallowed by Section 6(1),[44] it could potentially fit within the scope of deemed consent rules outlined in Section 7. While navigating the possibilities of data-sharing, one must not overlook the risks posed to data privacy by indiscriminate sharing of user data among companies, especially considering the importance of merger control in competition laws.

Once data sensitive markets have been identified, the next task is to establish a regulatory framework that redresses potential market failures. Here, the author suggests few observations from *Prufer's* article.[45] He argues that in *data-driven markets*, competitors struggle to achieve a significant market share against *dominant firms* in absence of governmental interference. To address this, it is recommended to implement mandatory protocols for the sharing of user-data.

---

[39] International Bar Association 'The Data Act: new EU rules for data sharing' (*EY*, 8 November 2022) <https://www.ey.com/en_es/law/the-data-act-new-eu-rules-for-data-sharing> accessed 7 August 2024.

[40] Press Information Bureau, 'CCI imposes a monetary penalty of Rs. 936.44 crore on Google for anti-competitive practices in relation to its Play Store policies' (*PIB*, 25 October 2022) <https://pib.gov.in/PressReleasePage.aspx?PRID=1870819#> (accessed 27 June 2024).

[41] Anuj Bhatia, 'Google's Android changes after CCI order: Four ways in which users get more control' *The Indian Express* (29 January 2023) <https://indianexpress.com/article/technology/google-policy-changes-4-ways-in-which-android-will-now-give-users-more-control-8406132/> (accessed 27 June 2024).

[42] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 6.

[43] ibid s 7.

[44] ibid s 6 (1).

[45] Jens Prüfer, 'Mandatory Data Sharing: Development of a Test & Governance Structure' (*Jens Prüfer*, 4 February 2021) <https://prufer.net/2021/02/04/mandatory- data-sharing-development-of-a-test-governance-structure/> accessed 8 August 2024.

In this light, *Prufer* recommends only *raw data* that can be stored almost free of charge should be shared. Such data is generated automatically when users interact with a provider. The analysis and processing of this data should be the responsibility of the recipient.[46] For example, in the search engine market, this would correspond to *search log data*. Providers with a market share of at least 30% should be obliged to share their user-generated data. This means that there would be a maximum of three providers per market that would have to share data. This figure would go down with increase in the degree of market monopolization.[47]

SEGMENTATION OF CONSENT: A LEAF FROM EU'S DIGITAL MARKETS ACT

The author supports *state enforced responsible data-sharing between tech giants* as a valuable solution in curbing anti-competitive data collection. However, when contemplating mandatory data-sharing as a solution to combat anti-competitive data extraction, an immediate concern arises about ensuring the responsible implementation of this practice and preventing it from inadvertently fostering uncontrolled anticompetitive mergers. This critical policy decision goes beyond the scope of this work. Nevertheless, the author aims to express views on a specific aspect related to this issue - data sharing under anti- competitive mergers.

In 2019, the German Federal Cartel Office looked into the competition implications of merging user data from one social media platform with that of another. This decision of the Federal Cartel Office was appealed against in the Court of Justice of the EU ("**CJEU**"), which, in July 2023, upheld the decision of the German Competition Authority.[48] The result of this judgement is that in Europe, competition authorities can now make an assessment as to whether or not there has been an abuse of the dominant position of a given entity based on a determination of whether or not the latter has acted in a manner consistent with its obligations under the GDPR.[49] European legislators had already chosen this path even before the CJEU's appeal ruling. The Digital Markets Act, a new legislation targeting competition matters in data-driven markets, includes a provision explicitly prohibiting designated *gatekeeper* online companies from merging user data without clear consent.[50]

In reaching its final decision,[51] the German Cartel Office emphasized the critical importance of obtaining separate consent for merging data, distinct from users' agreement to standard terms and conditions. The bundling of consent in this instance led the Office to confidently rule that the company had abused its dominant position and violated EU's data protection law.

In India, however, the conspicuous absence of a comparable provision in the Act to procure distinct explicit consent in scenarios that may potentially result in anti-competitive data aggregation is evident. The incorporation of such a provision within the ambit of the Act would have undoubtedly secured enhanced congruity between the regulatory aspects of competition

---

[46] ibid.

[47] ibid.

[48] Adam Satariano, 'Meta Loses Appeal on How It Harvests Data in Germany' *The New York Times* (4 July 2023) <www.nytimes.com/2023/07/04/business/meta- germany-data.html> accessed 22 July 2024.

[49] Rahul Matthan, 'Let's not have regulatory Overlaps on Data Compliance' (*mint*, 11 July 2023) <https://www.livemint.com/opinion/online-views/lets-not-have- regulatory-overlaps-on-data-compliance-11689089543845.html>.

[50] European Commission, 'DMA rules for digital gatekeepers to ensure open markets start to apply' (*European Commission*, 2 May 2023) <https://digital-markets- act.ec.europa.eu/dma-rules-digital-gatekeepers-ensure-open-markets-start-apply- 2023-05-02_en> accessed 9 August 2024.

[51] *Meta Platforms Inc. v Bundeskartellamt* Case No C-252/21 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A62021CC0252> accessed 22 July 2024.

and the framework of privacy. An explicit legislation on the competitive implications of data like the Digital Markets Act, is of course, not present. A significant number of legal disputes have arisen due to conflicts over jurisdiction between the commission and bodies such as the Telecom Regulatory Authority of India ("**TRAI**")[52] and Controller of Patents.[53] Regrettably, this oversight signifies yet another instance where the potential to avert conflicts between the esteemed entities of Data Privacy Authorities and Competition Regulators remains unrealized.

Therefore, it becomes essential to have policy discussions regarding the introduction of a specific provision in the Act, that mandates obtaining separate consent in cases of potentially harmful mergers. This provision should be distinct from the general terms of service for using a product and must not be subject to nullification by the exceptions provided in the deemed consent clause (Section 7) of the Act.[54] Defining the scope of *potentially harmful mergers* in this context, would once again constitute a crucial policy decision. Nonetheless, implementing such a provision would signify a departure from the compartmentalized approach towards privacy issues and anti- trust concerns, a welcome change as emphasized in the author's critique of the *Wolfgang-Zolna* Model discussed in the preceding sections.

CONCLUSION: LINKING AI ADVANCEMENTS TO THE PROPOSED ARGUMENTS

The core argument of this paper has been that achieving simultaneous market efficiency concerning *data privacy protection* and *market competitiveness* requires integrating the two policy tools (competition laws and data protection laws). Treating them separately cannot lead to the desired *second best* outcome due to significant overlap between the two domains.

The proposed solution by the author has been the establishment of a responsible and state-enforced system of *mandatory data-sharing* between big tech companies and new or emerging players in the market, as highlighted by the October 2022 Order of the CCI. Here, the author prefers the mechanism propounded by *Prufer*. Meanwhile, it is essential to distinguish this practice from indiscriminate data-sharing resulting from big tech mergers, as demonstrated through the analysis of the *German Meta* judgement.[55] While the former can be done through changes in the competition laws, the latter can only be achieved through relevant amendments in the Act.

The relevance of this line of reasoning becomes apparent in light of the advancements in AI.[56] The Act under Section 8(7)[57] provides that a data fiduciary should promptly discontinue the retention of personal data when it is reasonable to believe that the collected information no longer serves its original purpose and retaining it is no longer essential for legal or business reasons.[58] The illustration appended to the provision makes the philosophy behind the law evident. The same

---

[52] Rajvansh Singh, 'Supreme Court of Jurisdictional Conflict Between CCI and TRAI' (*IndiaCorpLaw*, 28 January 2019) <https://indiacorplaw.in/2019/01/supreme-court-jurisdictional-conflicts-cci-trai.html> accessed 6 August 2024.

[53] Essenese Obhan and Sneha Agarwal, 'CCI has Jurisdiction When Patent Rights are Abused: Delhi High Court' (*Mondaq*,27 July 2020) <https://www.mondaq.com/india/patent/969550/cci-has-jurisdiction-when-patent- rights-are-abused-delhi-high-court>.

[54] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 7.

[55] *Meta Platforms Inc. v Bundeskartellamt* Case No C-252/21 <https://eur- lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A62021CC0252> accessed 22 July 2024.

[56] The term "Artificial Intelligence" under this section has been used as an umbrella term encompassing related technologies like Machine Learning, Deep Learning, Unsupervised Learning, and Artificial Neural Networks.

[57] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 8 (7).

[58] The Digital Personal Data Protection Bill, 2022, s 9(6).

is reproduced herein." *'A' creates an account on 'Z', a Social Media Platform. As part of the process of creating the account, 'A' shares their personal data with 'Z'. After three months, 'A' deletes the account. Once 'A' deletes the account, 'Z' must stop retaining the personal data of 'A' or remove the means by which the personal data of 'A' can be associated with 'A'.*"

The example above presents a simplistic scenario where a company seeks access to a consumer's personal data in order to offer them a service. It assumes that the data is solely used for business purposes related to that individual. However, the true nature of data utility is far more multidimensional. Undoubtedly, information is necessary for identity verification, delivering relevant content, and providing immediate consumer benefits. Yet, data collection also serves a crucial purpose in *data analytics* and *algorithm development*. Companies require access to information to understand user behaviour, enabling them to create superior products in the long run. This aspect is undeniably of greater importance from the point of view of competition law as it provides a larger market advantage than the ability to serve a singular user.

While data analytics is not anything new, emergence of AI-powered data analytics brings challenges to algorithm transparency. Complex models like deep learning neural networks make it difficult to understand their inner workings.[59] In an era where corporations extensively train their AI systems on internet content with little regard for intellectual property rights,[60] it is unrealistic to expect them to show hesitation in leveraging legally accessible data for the same purpose. Once an AI model gets trained on the data of a particular user, the information would continue to exist as part of the model eternally. Deletion of user data after that point would have no impact on the final algorithm or the accrued competitive advantage.[61]

As Artificial Intelligence and allied tools make subsequent data deletion redundant, enforcement of responsible data-sharing along with segmentation of consent at instances where the same is required, offers a solution that ensures robust market competition along with quality product delivery. This model of integration between the competition laws and data privacy frameworks is the only feasible solution to the deal with the probable perils of rapid changes in the digital market.

[59] Heike Felzmann et al, 'Towards Transparency by Design for Artificial Intelligence' (2020) 26 Science and Engineering Ethics <https://link.springer.com/article/10.1007/s11948-020-00276-4> accessed 9 August 2024.

[60] Catherine Thorbecke, 'Google Hit with Lawsuit Alleging It Stole Data from Millions of Users to Train Its AI Tools' *CNN* (12 July 2023) <https://edition.cnn.com/2023/07/11/tech/google-ai-lawsuit/index.html> accessed 17 July 2024.

[61] Catherine Tucker et al, 'Privacy, Algorithms and Artificial Intelligence' in Josh Lerner and Scott Stern (eds), *Innovation Policy and the Economy* (Vol 21, University of Chicago Press 2021) <https://www.nber.org/system/files/chapters/c14011/revisions/c14011.rev1.pdf> accessed 9 August 2024.

Citation: Shilpa Khandelwal, 2024. "Harmonizing Competition Regulations and Data Privacy Laws in the Era of Artificial Intelligence". International Journal of Academic Research, 11(3): 184-196.

https://doi.org/10.5281/zenodo.13983084