



## The Importance of China's Competition Law in the Management of Data in the Country's Rapidly Developing Digital Economy: Policy Recommendations for Pakistan

Shahzada Aamir Mushtaq<sup>1</sup>, Khurram Baig<sup>2</sup>, Saifullah Hassan<sup>3</sup>, Waqas Ahmad<sup>4</sup>

<sup>1</sup> Assistant Professor, Department of Law, Times Institute Multan, Pakistan. Email: amirqureshi.adv@gmail.com

<sup>2</sup> PhD Scholar University Gillani Law College, Bahauddin Zakariya University Multan, Pakistan.

Email: mkb5729@gmail.com

<sup>3</sup> Lecturer, College of Law, University of Sargodha, Pakistan. Email: saifullah.hassan@uos.edu.pk

<sup>4</sup> LLM Gillani Law College, Bahauddin Zakariya University Multan, Pakistan. Email: waqas1816@gmail.com

### ARTICLE INFO

#### Article History:

Received: December 26, 2023

Revised: February 10, 2024

Accepted: February 11, 2024

Available Online: February 12, 2024

#### Keywords:

Digital Economy

Data Regulation

Internet Industry

Competition Law

Regulatory Competition

Neo-Protectionism

Innovation

#### Funding:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

### ABSTRACT

With the expansion of the digital economy and the rising importance of data, organizations are under more regulatory scrutiny over the collection, use, and sharing of data. Antitrust and competition authorities and governments worldwide are now evaluating and deliberating on the applicability and suitability of antitrust and competition laws in addressing data-related issues, notably within the digital economy. Parallel ideas and concerns are also gaining prominence in China. China has not only been enhancing its legislative framework to govern and facilitate state control over data, but it has also significantly strengthened regulatory oversight and control over Internet and technology firms. Competition legislation has prominently featured in China's governmental efforts to suppress the Internet and technology industries. Regulatory competition in the post-industrial digital economy is examined. Regulatory competition is achieved through neo-protectionism, which aims to boost social and economic development and growth by creating new comparative advantages in the digital economy. Innovative, digital, and information Neo-protectionism has emerged as a key aspect of international economic strategy for nations that lead its implementation. This article examines how China's competition laws may regulate Internet and technology companies' data and behavior. By analyzing China's data regulatory structure and competition rules, including political and economic aspects, this is achieved. China's political economy and competition rules consider many interests, aims, and priorities. Concerns that other nations may not associate with competition law may be included. China's macroeconomic monitoring guides competition law enforcement.



© 2024 The Authors, Published by iRASD. This is an Open Access article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: [mkb5729@gmail.com](mailto:mkb5729@gmail.com)

**Citation:** Mushtaq, S. A., Baig, K., Hassan, S., & Ahmad, W. (2024). The Importance of China's Competition Law in the Management of Data in the Country's Rapidly Developing Digital Economy: Policy Recommendations for Pakistan. *Current Trends in Law and Society*, 4(1), 27-51. <https://doi.org/10.52131/ctls.2024.0401.0030>

## 1. Introduction

The significance of digital marketplaces in contemporary society has witnessed a corresponding increase in the quantity and diversity of data that have been created, gathered, utilized, and exchanged. The capacity to obtain, manage, evaluate, and utilize data is becoming progressively more crucial for businesses, particularly those functioning within the realm of the digital economy. Simultaneously, there has been an increase in

regulatory and political examination of the data and data practices employed by firms. TikTok, owned by Chinese corporation Byte Dance, has been under governmental and public criticism in the US. Concerns that the Chinese government may access user data have prompted this inquiry. Thus, privacy, security of data, cyber security, and national concerns have arisen (Wendy Hodsdon & Zwickey, 2010; Zhi et al., 2024).

Likewise, the issues of data and data practices are of utmost importance in the discourse on competition law pertaining to the governance of digital platforms. Competition authorities and legislators worldwide are currently engaged in discussions and debates regarding various inquiries. These inquiries encompass the impact of data on market definition as well as the evaluation of market strength and competitive effects. Additionally, there is deliberation on the potential anticompetitive nature of data-based business approaches and practices. Furthermore, the incorporation of privacy and data protection concerns within competition law frameworks is also a subject of consideration. In February 2019, the Bundeskartellamt (German Federal Cartel Office) of Germany issued a significant ruling, determining that Facebook had violated German competition regulations through its practices of gathering, analyzing, and utilizing data pertaining to users and their devices. This represents the inaugural instance in which a competition watchdog has predicated a violation of competition law on the grounds of non-compliance with privacy and data protection legislation. Competition legislation and other legislative reforms have also focused on data and data practices, with the aim of implementing *ex ante* regulation for digital platforms. These measures have either been enacted or are now under consideration (Ezrachi & Stucke, 2023; Han et al., 2024).

The information and data practices of firms in China have also garnered political and regulatory scrutiny. In recent years, China has been actively establishing a comprehensive legal framework to effectively govern and facilitate the state's authority in managing data. Cyber security, data security, and personal data protection are covered by this framework. After slack regulatory monitoring and limited control over internet and technology businesses, which prioritize innovation and growth above regulation, China has increased regulatory inspection and control over the industry. Ant Group's highly anticipated IPO (initial public offering) was suspended by the Shanghai Stock Exchange in November 2020. A financial technology subsidiary of Alibaba, just before securities trading began, marked a turning point in China's political and regulatory landscape for large internet and technology companies and the sector as a whole. The Chinese government took several steps to discipline Alibaba, a large online conglomerate. Additionally, it initiated a comprehensive regulatory and enforcement campaign that focused on the internet and technology sectors (Liu, Zheng, Li, & Ma, 2020; Singh et al., 2023; Wang et al., 2024).

Chinese regulatory authorities have implemented measures to address some companies and have introduced a comprehensive set of regulations to oversee the operations of organizations engaged in the digital economy. The campaign has addressed a wide array of topics and issues, encompassing sectors such as data, regulation of finance, cyber security, labor, transport, video games, online education, fan culture, and income redistribution, among others. Competition legislation has been prominently featured in the context of this campaign (Ezrachi & Stucke, 2023).

This article investigates the potential use of China's competition laws in regulating the data and information techniques employed by firms operating within the digital economy. This study conducts a political economy and specific analysis of China's data regulation framework, examining its interplay and interdependence with China's competition laws. China's political economy and competition laws, which take into account a variety of interests, goals, and priorities, have an impact on the enforcement of competition law in that nation. These considerations may extend beyond what other jurisdictions typically address under competition law. The state provides macroeconomic supervision and guidance in this enforcement process (Djalilova, 2023).

The present article is organized in the following manner: In the first part, an analysis is conducted on the regulatory framework pertaining to data in China. This section not only examines the established legal framework governing data regulation but also elucidates the various interests, concerns, and objectives held by the state, enterprises, and the public with regards to data. The text additionally examines the many methods employed by the

state to exert control over the primarily privately owned internet and technology enterprises operating within China. It also delves into the political issues surrounding the administration of data. The second part of this study investigates the use of China's competition laws in the regulation of enterprises' data and data practices. This article compares China's data governance framework to competition legislation and analyzes the potential impact of this link on the enforcement of competition laws in Part III. The fourth section draws to a conclusion.

## **Part A: Literature Review**

### **2. China's Data Regulatory Environment**

The Chinese government employs several mechanisms to regulate, monitor, and oversee the collection, access, utilization, exchange, and transfer of data. By doing so, the state aims to achieve a delicate equilibrium between the commercial interests of the entities involved in data collection and management, privacy relating to data providers, and its own data interests (Caglar, Daştan, & Rej, 2024).

This section first summarizes the state's different data interests and difficulties. The subsequent section of this paper examines and evaluates the existing legislative structure governing data governance. It specifically explores the manner in which this framework strives to strike a balance and satisfy various concerns, objectives, and vested interests held by people, businesses, and the government with regards to data. The state uses official and informal measures to control and influence dominant private firms in the digital economy, in addition to data governance standards, which will also be examined in this discussion. This section examines the political processes and considerations that emerge in the realm of data governance. The essay does not delve into the potential ramifications of China's data governance system outside its domestic boundaries (Ezrachi & Stucke, 2023; Khan & Liu, 2012).

#### **2.1. Interests of the State in Data**

With regard to China, data is regarded from a dual perspective, encompassing both the potential opportunities it offers and the associated threats it entails. This particular point of view has a big impact on the way the state controls data. Data play a crucial role in the achievement of the state's objectives and interests related to national security, public security, and economic and social growth. Furthermore, the advent, progression, and widespread adoption of the internet have had a significant impact on the state's perspective on data and its governance. This is primarily due to the increased accessibility, sharing, and communication of information, the rapid growth of the digital economy, and the generation of vast amounts of data. The intertwining of internet regulation and data regulation has become a significant aspect (Glass & Tardiff, 2023; Zhang & Qu, 2024).

Political and national security considerations are the main factors influencing China's approach to data analysis. Throughout history, the state has exerted significant control over the flow of information and its many channels of distribution, with the aim of mitigating potential political instability. The entity engages in proactive censorship and regulation of media content, possesses ownership of conventional media platforms, and exercises regulatory control over periodicals and other media channels. China possesses a robust propaganda apparatus and actively partakes in proactive propaganda endeavors, entailing the generation and dissemination of material deemed essential for public awareness. The advent of the internet has significantly magnified the implications of data in the realms of politics, national security, and sovereignty. This is mostly attributed to the internet's facilitation of enhanced accessibility and communication of information, hence presenting novel challenges and risks to the authority wielded by nation-states. The internet has assumed a crucial role in safeguarding China's security and sovereignty. Consequently, the government employs a diverse range of technological and legal strategies to oversee, govern, restrict, and suppress the flow of information accessible and disseminated online, as well as regulate the channels through which such data can be obtained and circulated, along with other online activities. Simultaneously, data holds significant importance in relation to China's economic and developmental objectives (Spulber, 2023).

The state regards data as valuable economic resources. Data is considered a factor of production, and the establishment of a market for data factors is crucial for facilitating the advancement of high-quality development. In a similar vein, big data is perceived as a crucial strategic asset. It is noteworthy that various regulations have been implemented to foster the growth of big data companies. Moreover, a significant number of China's pivotal development strategies heavily depend on solutions generated by big data. Data play a crucial role in China's information technology policy, which aims to transition the economy, society, and governance towards being technology-driven. Moreover, there is a growing trend in which the nation is utilizing data to bolster and revolutionize its operations, including but not limited to law enforcement, monitoring, societal regulation, and the provision of public services. China is currently engaged in the development of strategies pertaining to "social credit," which involves the utilization and integration of technology and digital data. The objective is to enhance economic and social order as well as foster trust among individuals. Additionally, China is intensifying the exchange of data between governmental entities and digital platforms. This facilitates the collection of market and business information, as well as the implementation of e-government initiatives (Caliskan, Açıklkalp, Rostamnejad Takleh, & Zare, 2023).

## **2.2. Legal Framework for Data Regulation**

China's main data laws include the Cyber Security Law, the Data Privacy Law, and the Private Information Protection Law. The aforementioned regulations serve as the fundamental principles inside China's legal infrastructure for the regulation of data. The three laws control data differently, aligning with the state's data interests, corporations' financial interests, and individuals' privacy concerns. Data is governed by the Cyber security Law to protect digital and national security, cyber sovereignty, general public interests, and the lawful rights of people, legal bodies, and other organizations. It also promotes economic and social digitization. The Data Security Law regulates data to protect supremacy and national security, grow data as well as data-related companies and technology, promote the digital marketplace, and protect individuals' and organizations' data rights and interests. The law's main goal is to protect people's personal data. In a similar vein, it should be noted that the nature of the data subject to regulation varies across each respective statute. The Data Security Law has the widest jurisdiction, encompassing all types of information records, regardless of their format, while the Cyber security Law specifically governs computer networks and private information. On the other hand, the Personal Information Protection Law exclusively pertains to personal information (Abada & Lambin, 2023).

In general, the data governance framework primarily centers on the responsibilities of enterprises and, to a lesser degree, governmental entities in relation to data. These requirements can be classified into various overarching categories. Primarily, the above requirements protect systems and operating data. Organizations must implement data security management structures, and "crucial data" handlers must frequently review their data handling risks. Additionally, they are required to assign designated individuals and management bodies to assume responsibility for fulfilling their data security obligations. Network operators are obligated to implement specific safeguards aimed at mitigating the risks of data leakage, theft, and falsification within their networks. It is imperative for operators of key information infrastructure to prioritize the security of their networks and store significant data or private information within the boundaries of China. In the same vein, it is imperative for state authorities to build a comprehensive data security management system, effectively implement data security safeguard tasks, and diligently safeguard government data to maintain its security (Wach et al., 2023).

Data governance also separates various data types. Data are classified by their importance for social and economic advancement and the risk of unsanctioned modification, destruction, leakage, or acquisition and use for public welfare, national security, or an individual's or organizations legal rights. Specifically, data will be considered "fundamental data of the state" when it pertains to matters of national safety, the crucial foundation of the country's economy, significant facets of individuals' well-being, and substantial public concerns. The classification of data has implications for the extent of security measures applied to safeguard the data, the manner in which data is handled, and the applicability of laws concerning outbound security management and data localization. For example, a

stricter management structure applies to the state's major information assets. Furthermore, network data categorized as "important data" gets heightened safeguards, necessitating its storage within the borders of China. Additionally, outbound security management measures are in control of these data.

Within the framework of data regulations, additional restrictions, safeguards, and oversight are applicable to personal information. There are three key distinctions between the ways in which data governance regulations handle personal information. Personal information is subject to regulation and protection, acknowledging its significance to individuals as well as the nation. The Personal Data Protection Law and the Cyber security Law share with individuals a certain level of authority and safeguard in relation to their personal information. The acquisition, utilization, and management of personal data necessitate the explicit consent of individuals, a consent that can subsequently be retracted and revoked. Individuals also have the ability to retrieve and duplicate their personal data, as well as make a formal request for the transfer of their personal information to another entity. Furthermore, they possess the right to rectify any inaccuracies present in their personal data and request the deletion of unlawfully obtained or mishandled personal information. Important personal information is granted additional safeguards and subjected to more stringent limitations compared to other forms of personal information (Kölbel, 2023). Moreover, in cases in which automated decision-making is employed and significantly impacts an individual's interests and liberties, persons possess the entitlement to demand an elucidation from the company about the choice, and they also have the right to object to the use of automated decision-making tools for that decision. Simultaneously, the safeguarding of personal information is upheld by the Cyber security Law as a crucial element in the preservation of network information security. Additionally, there are limitations on the transfer of personal data to foreign jurisdictions, and certain enterprises and governmental entities are required to store the personal data they acquire and manage inside the borders of China.

Furthermore, businesses assume crucial functions in the regulation of personal information. Individuals rely on them as the main safeguard for the protection of personal information, as data governance rules primarily focus on mitigating the commercial risks connected with the acquisition, utilization, and management of personal data. In order to comply with legal regulations, businesses are obligated to acquire explicit consent from individuals prior to collecting, utilizing, and managing their personal information. Additionally, businesses are required to furnish individuals with specific information prior to handling their personal data. Moreover, businesses are expected to employ technical as well as other measures to safeguard personal data and mitigate the risk of unauthorized entry, communications, theft, interference, and loss of personal data. In addition, individuals are forbidden from engaging in the sale or unauthorized provision of personal information to third parties, as well as the collection or handling of personal information that exceeds the necessary scope or is unrelated to the services rendered. Furthermore, the unauthorized acquisition or theft of personal information, as well as the disclosure or tampering with such information, is strictly prohibited. In instances where businesses employ personal information for automated decision-making processes, it is imperative that they refrain from engaging in unjustifiable discriminatory practices. Furthermore, if such information is utilized for the purpose of conducting information push delivery or commercial marketing, businesses are obligated to offer non-tailored alternatives and the choice to decline participation. Moreover, many digital platforms are obligated to actively oversee the management of personal information within their systems (Edwards et al., 2023).

Furthermore, it seems that the data governance regulations do not impose substantial limitations on the state's capacity to obtain, regulate, and utilize personal data. State authorities that obtain or use personal information for legal purposes have limited obligations. Individuals must ensure that personal data collection and use are limited to their roles. Furthermore, they must uphold the confidentiality of any personal information encountered during the execution of their duties, refraining from disclosing or unlawfully disseminating such information to external entities. Additionally, individuals are obligated to furnish specific information to the concerned individuals. In addition to the aforementioned obligations, it remains uncertain whether state authorities are obligated to adhere to the same requirements as other entities responsible for managing personal information.

However, it is worth noting that the Personal Information Protection Law explicitly states that consent is not required for the collection, handling, or utilization of personal information when it is deemed necessary to fulfill statutory responsibilities, duties, and obligations. Moreover, instances pertaining to national security and sovereignty, public safety, the well-being of the public, substantial public welfare, criminal investigations and enforcement, emergencies, media coverage, public opinion control, and analogous activities in the interests of the public do not necessitate consent. These situations frequently fall under the purview of state authorities' responsibilities (Roberts, 2023).

This analysis demonstrates that the data regulation legislative framework effectively incorporates national security, public safety, the benefit of society, construction, businesses, and data privacy. This phenomenon is particularly emphasized in the manner in which personal information is governed in accordance with data governance legislation. The data governance system not only addresses the increasing consumer expectations for private information liberties and safeguards, but it also does so in a way that minimally restricts the state. The fact that corporations take on the majority of the commitments and restrictions facilitates the simultaneous effort to achieve these two seemingly incompatible objectives. Furthermore, it is important to note that data governance rules acknowledge the possibility that personal information can be considered a public asset, carrying potential consequences for national security, public security, and overall societal progress. Consequently, such information may be subject to regulation in accordance with these considerations.

The complex administrative enforcement procedures that support data regulation reflect complex concerns, goals, and interests. The Cyberspace Administration of China plans, coordinates, supervises, and manages cyber security initiatives under the Cyber security Law. Within their duties, the Ministries of Industry and Information Technology (MIIT) and Public Security (MPS) protect, monitor, and manage cyber security. The Central Leading Authority on National Security, CAC, MPS, MSS, and regional regulatory agencies execute the Data Security Law. These organizations manage data gathering and security in their areas. According to the Personal Information Protection Law, the CAC organizes plans, manages, and supervises the country's data protection operations. The legislation also requires government departments to preserve, supervise, and manage personal information within their jurisdictions and duties (Funta, 2012).

The aforementioned enforcement arrangements serve to underscore the heterogeneity of the state's objectives, apprehensions, and vested interests pertaining to data. The scope of entities participating in managing data is extensive, and none of them prioritizes data governance as their main area of concern. The China Administration of Cyberspace (CAC) assumes the responsibility of overseeing cyber security, information technology, and online content governance. The Ministry of Industry and Information Technology (MIIT) serves as the regulatory body for the information technology and telecommunications sectors. The Ministry of State Security (MSS) is entrusted with safeguarding national security, including political and domestic aspects, as well as conducting intelligence-related activities in China. Lastly, the Ministry of Public Security (MPS) is liable for maintaining law and order, enforcing criminal laws, and ensuring public security. The enforcement of data governance is characterized by both horizontal and vertical dispersion. Horizontally, it involves departments, ministries, and party officials with different functions. Vertically, it spans government tiers and regions. Thus, many national and provincial state bodies participate in data governance. Different origins and jurisdictions of various authorities may lead to different data and data administration perspectives and methods. Thus, data-related inconsistencies, disagreements, and disputes within the state may result (Li, Wang, Cheng, & Song, 2023).

## **Part B**

### **3. Alternative Methods of State Influence and Control**

Data governance laws allow the Chinese government to directly monitor internet and technology companies' data and practices. The state has several legal and informal ways to regulate and access internet and technology companies' data. Private enterprises have driven China's digital economy's growth and innovation. The nation's top internet and technology companies are privately held. The Communist Party of China has explicitly

expressed its intention to enhance its authority and impact on private enterprises and entrepreneurs in order to further its political objectives and mitigate the unregulated growth of capital.

Compliance with rules and laws is a fundamental need for accessing China's substantial market. This requirement is universally applicable and entails that both Chinese and non-Chinese technology and internet companies, regardless of their ownership structure, are obligated to adhere to rigorous regulations pertaining to censorship and information control. Furthermore, these companies are expected to contribute to the preservation of China's national security and actively participate in and facilitate national intelligence endeavors. Companies that fail to adhere to these stipulations, which pertain to their data collection, sharing, and handling practices, are prohibited from accessing the Chinese market. In 2010, Google withdrew its search engine services from China for violating China's censorship laws. Apple, however, stores data in mainland China and complies with censorship orders. The state encourages internet and technology businesses to seek data with standards and other help. The state's development strategies favor the internet and related IT businesses. The "Internet Plus" Action Plan, Made in China 2025, and National Informatization Development Strategy are key Chinese programs (Dong, Wang, Sun, Fan, & Lu, 2023).

These rules assist Chinese internet and IT enterprises' growth, aligning with the government's goal of becoming a worldwide online leader. China wants many competitive global internet and IT enterprises by 2025. These important projects and policies use and enhance data. Companies that proactively utilize their data to develop technology aligned with governmental goals should expect to gain advantages, including enhanced financial accessibility, incentives, and a generally more advantageous regulatory landscape. Moreover, enterprises that are classified as "national champions" or participants of the "national team" receive additional advantages and privileges, such as financial assistance and other forms of support, to facilitate their expansion and enhance their competitiveness on the global stage. This status grants these companies advantageous advantages, encompassing standard-setting authority and safeguarding against challenge from government-owned industries. Consequently, these state legislative efforts align internet and technology corporations' data economic interests with those of the states, minimizing the disparity.

The country possesses the capability to exert influence and oversee the data and operations of technology and internet corporations from an internal standpoint. Although several Chinese internet and technology companies operate under private ownership, the state maintains a degree of involvement within these private enterprises. By the conclusion of 2016, approximately 68% of Chinese private enterprises had successfully formed party committees. Moreover, it is widely speculated that this proportion is significantly greater among prominent Chinese internet and technology firms. All of China's top 100 online businesses have formed party committees, according to the reports that are currently available. Tencent, Alibaba, and Baidu have reportedly been required to put party membership on their boards because of their size and influence. Several significant Chinese internet and technology companies are led by the National People's Congress and Chinese People's Political Consultative Conference members. There have been rumors indicating that the government is engaged in discussions on the acquisition or has already acquired minor ownership stakes in several prominent internet corporations. These advancements indicate a growing correlation between private internet and technology corporations and the government in terms of political affiliations (Wu & Philipsen, 2023).

Despite the existence of data governance legislation and other regulatory mechanisms, the state's ability to manage data is not comprehensive or indisputable. For example, the Chinese state exhibits a lack of homogeneity, uniformity, and monolithic characteristics. The state bureaucracy exhibits fragmentation, wherein diverse state entities, operating centrally and locally, may possess divergent and contradictory goals as well as political and economic motivations. This phenomenon may lead to a lack of implementation of centrally established policies at the local level as well as the emergence of power dynamics between various agencies and provinces. These power struggles may encompass issues related to regulatory jurisdiction and data management. Moreover, it is

worth noting that internet and technology corporations do not consistently collaborate and adhere to requests made by governmental entities, particularly those pertaining to data accessibility. Despite the constrained scope for challenging or opposing the state's requests for data access and cooperation, there have been occurrences in which internet and technology firms have resisted the state's demands, altering degrees of effectiveness and repercussions (Bui, Nguyen, & Pham, 2023).

### **3.1. Data Governance and its Political Dynamics**

The legislative framework for data regulation is part of broader government procedures. That exerts influence and control. This framework serves as a platform for various stakeholders, both public and private, who possess diverse interests and objectives, which may not always align harmoniously. Resolution of data governance regime disputes, tensions, or contradictions, trade-offs, and stakeholder interactions, and the impact of power dynamics on results, are unpredictable. Coordination and harmonization of numerous stakeholders' agendas and interactions occur within the nation's power and regulation of the online economy and its players.

In order to elucidate certain political processes that may emerge in the realm of data governance, this section delves into an analysis of the Chinese government's enforcement effort, which specifically aimed at regulating the personal information practices of mobile phone applications. The CAC, MIIT, MPS, and SAMR started the App Personal Information Protection effort in January 2019. This collaborative enforcement effort aimed to resolve the issue of the unlawful use and gathering of individual data by mobile applications across the nation. The program was scheduled to last for one year. The campaign's main goal was to ensure and improve adherence to the obligations related to the protection of personal information as outlined in the Cyber security Law. The authorities identified, targeted, and corrected instances of network operators who were not in compliance with the Cyber security Law's requirements for protecting personal information. Furthermore, the China Administration for Cyber security (CAC) and the State Administration of Market Regulation (SAMR) collaborated to build a certification system for ensuring the security of personal information in mobile applications. Additionally, the Ministry of Industry and Information Technology (MIIT) aimed to enhance the network data security abilities of telecommunications and internet enterprises. The aforementioned agencies have jointly issued a pair of guidelines pertaining to the identification of illicit practices involving the gathering and utilization of personal data by mobile applications. In July 2020, the China Administration for Cyberspace (CAC), Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS), and State Administration for Market Regulation (SAMR) jointly declared the initiation of a subsequent enforcement campaign aimed at further advancing their collaborative efforts in combating the illicit acquisition and utilization of personal data by mobile applications (Funta & Ondria, 2023; Garces & Colangelo, 2023).

The App Personal Information Protection Campaign effectively encompasses a diverse range of interests, concerns, and goals, which are duly acknowledged and harmonized. The Chinese government acknowledges the significance of applications in advancing economic growth and meeting the demands of the people. Additionally, it recognizes that personal data is an essential, important, and lucrative asset for firms operating in the online economy. The three government agencies that are in charge of enforcing the Cyber security Law—the Cyberspace Administration of China (CAC), the Ministry of Public Security (MPS), and the Ministry of Industry and Information Technology (MIIT)—are all there. Their participation shows how they protect personal information based on their different views on cyber security, public security, and industrial policy. Furthermore, despite the absence of explicit obligations stipulated by the Cyber security Law, the SAMR actively participates in the App Personal Information Protection Campaign due to its role in upholding the Safety of Consumer Rights Act. The statement explicitly emphasizes that safeguarding private information serves as a method for safeguarding consumer interests.

Unlike traditional law enforcement, the Chinese government's campaign-style enforcement of app-related data collection and use provides valuable insights into the political dynamics of personal data protection and data governance. Firstly, it is evident that the preservation of personal information enjoys substantial political backing and



prominence. According to Benjamin van Rooij's observation, political leaders initiate campaigns in response to situations that create a political imperative for action to be undertaken.

Furthermore, it is apparent that the Chinese government possesses a vested interest in ensuring that the general populace is aware of its commitment to safeguarding personal information and addressing the concerns expressed by the public. China is currently experiencing mounting apprehensions around theft, leakage, and improper utilization of personal data, particularly in online contexts. Furthermore, there is a rising public desire for enhanced safeguards pertaining to personal information. Enforcement campaigns exhibit a high degree of public visibility and frequently engage the participation of the general population. As a component of the App Privacy Awareness and Protection Initiative for 2019, individuals were actively encouraged to participate by submitting personal information, filing complaints, and sharing experiences of apps that violate privacy standards for user data. The outcomes of this campaign, including the assessment of numerous apps, identification of non-compliance, investigation of specific instances, and imposition of penalties, were extensively disseminated across various media platforms. The initiative helps the Chinese government demonstrate that personal data issues are being handled. This helps sustain public faith in government and legitimize leadership. The program would have helped China communicate information about its new personal data protection regulatory and legal framework. Furthermore, the Chinese government encounters bureaucratic obstacles when it comes to the regulation and safeguarding of personal information. The involvement of multiple government authorities in the implementation of the cyber security law has resulted in conflicts over jurisdiction, inconsistencies, and inefficiencies in enforcement. In recent years, the Chinese government has undertaken many endeavors aimed at consolidating control over cyberspace and internet-related endeavors in an effort to address the aforementioned difficulties. Enforcement campaigns serve as a pragmatic mechanism enabling the central government to exert immediate control over local governments, facilitate enforcement coordination among various government bodies, and surmount opposition from authorities that may otherwise exhibit reluctance towards enforcement efforts (Gauri, Rahman, & Sen, 2023; Goode, 2021).

Furthermore, the implementation of this campaign would have facilitated the government in effectively amassing, organizing, and deploying its constrained enforcement resources with a specific focus on addressing the safeguarding of private information.

### **3.2. The Data Pertaining to China's Competition Laws.**

The data governance framework in China has predominantly prioritized the mitigation of data risks pertaining to national security, public security, and privacy. It has also aimed to promote the utilization and advancement of data to support economic and developmental objectives. Simultaneously, the regime has imposed restrictions on commercial actions involving data while ensuring that the state continues to have access to and use of data. The explicit consideration of the influence of information and data management practices on competitiveness is currently absent from the existing data governance framework.

China has enacted two primary pieces of legislation that address various facets of competition. The Anti-Monopoly Law (AML) encompasses provisions that ban both horizontal and vertical monopoly agreements, as well as the abuse of market dominance and anticompetitive mergers. This legislation bears resemblance to the antitrust and competition laws observed in numerous other nations. Additionally, it serves to prevent anticompetitive practices stemming from the exercise of administrative authority. The Anti-Unfair Competition Law (AUCL) prioritizes economic fairness and corporate ethics among unfair competition practices. The State Administration for Market Regulation (SAMR) has implemented the AML and AUCL since March 2018. The State Anti-Monopoly Bureau implements the AML, while the Price Supervision and Inspections and Anti-Unfair Competition Commission enforce the AUCL. Private parties may also enforce AML and AUCL (Bourguignon, Faivre, & Turq, 2004).

### **3.3. Information Required by the Law Against Unfair Competition**

Data competitive effects under the AUCL have mostly been examined in private litigation. One firm steals data from another's website or digital platform in these circumstances. Article 2 of the AUCL was used to examine this behavior. Article 2 requires businesses to follow laws, business ethics, voluntariness, equality, fairness, and honesty. Courts have looked into the effects of unauthorized data collection and use on corporate ethics and economic interests.

When a business fails to obtain user consent from the data controller, user consent from the business seeking to collect and use the data, and data controller consent from that business, it violates Article 2 of the AUCL and business ethics. This failure includes taking user data from another company's website or platform for personal use. In a similar vein, it has been determined by courts that appropriating and using data in a way that threatens data security, violates data rights and interests (such as user privacy and personal information protection), negatively impacts a business's goods or services, undermines or impairs its competitive advantage or commercial incentives, or violates applicable rules and regulations (such as the Cyber security Law) is unfair. This is because it harms company interests and violates commercial ethics.

In these cases, courts have distinguished between two types of digital platform data: the comprehensive data resource and the data pertaining to individual entities. Furthermore, they have examined the consequences of both categories in relation to unfair competition. The digital platform possesses ownership of the comprehensive data resource due to its investment in resources. However, the data generated by individuals remains the property of those individuals. Consequently, the digital platform is only permitted to utilize this data in compliance with its user agreement and the principles of necessity, permission, and lawfulness. The judiciary has ruled that despite the infringement upon user data rights, the unauthorized acquisition and utilization of such data by a third-party entity can still constitute a violation of the AUCL. This is due to the detrimental impact it has on the digital platform's competitive edge and business gains from owning the comprehensive data repository (Schneider, Kamal, Jin, & Schölkopf, 2023).

## **Part C**

### **4. Anti-Monopoly Law Data**

The consideration of data and its associated concerns regarding its influence on competition has been undertaken in relation to misuse of dominance, mergers, and monopolies, but to differing extents. Historically, the consideration of statistics in abuse of power instances has been a relatively new development. In the case of Qihoo 360 v. Tencent, the Supreme People's Court examined whether Tencent had violated Article 17(4) of the Anti-Monopoly Law (AML) by their tying activity. During the evaluation, the court briefly acknowledged data privacy as part of product and service excellence and a legitimate reason for such activity.

The aforementioned change took place in response to the SAMR's identification of recent instances of abuse of dominance on digital platforms, specifically Alibaba and Meituan. In these instances, while the focus of the investigation was not primarily on data, data played a significant role in delineating the pertinent markets, establishing market dominance, identifying instances of dominant behavior, and forming the obligations that Alibaba and Meituan were obligated to fulfill. The discernment made by the SAMR on the non-equivalence of online and offline services within the relevant market was primarily influenced by the online platforms' capacity to analyse and leverage data for the purpose of augmenting their services (Colangelo et al., 2023).

The State Administration for Market Regulation (SAMR) found that Alibaba and Meituan dominated their marketplaces due to their large data sets and ability to analyze, process, and exploit them. These technological and competitive advantages have strengthened their market power. The SAMR (State Administration for Market Regulation) also recognized data, data systems, and algorithms as platform infrastructure components that hindered market access. Additionally, it also acknowledged that data cost customers switching as businesses encountered difficulties in transferring the accumulated data from

one platform to competing platforms. In its assessment of abusive conduct related to dominance, the State Administration for Market Regulation (SAMR) determined that Alibaba and Meituan, among other actions, employed data, algorithms, and various technical methods to survey and enforce compliance with platform regulations by their consumers. Consequently, this practice hindered customers from engaging with competing entities. Moreover, Alibaba and Meituan were required to fulfill certain pledges pertaining to their data and practices. These two companies were instructed to refrain from utilizing data, algorithms, platform regulations, and many technical methods to establish monopolistic promises, partake in abusive dominant behavior, and impede or limit competition. Additionally, they were urged to prioritize the safeguarding of personal information and privacy. Meituan, in particular, was specifically directed to abstain from engaging in the unlawful collection of personal information. Alibaba was additionally requested to utilize its data resources in an equitable and unbiased manner while also improving the accessibility of the data interface on its platform. Recently, a notable instance of private litigation pertaining to data protection under the Anti-Monopoly Law (AML) occurred. Sina Weibo, a prominent social media platform in China, faced a lawsuit alleging the misuse of its dominant position by denying data access to others (Bergqvist & Choi, 2023).

Concerns regarding data have also been raised in several cases involving mergers and agreements related to monopolies. It is worth noting that the majority of these lawsuits did not involve digital market companies. One of the primary issues regarding struggle that has been highlighted during the process of reviewing mergers is the potential for the acquiring company to obtain access to specific data as a result of the merger. This access might potentially provide the acquirer with both the capability and motivation to utilize the data in a manner that would negatively impact competition. In order to address these concerns, the parties involved in the merger have made agreements to provide data accessibility, impose limitations or prohibitions on data transmission and sharing, and implement measures aimed at safeguarding data. The transmission of information between various entities, whether in written or spoken form, utilizing official and informal, as well as direct and indirect channels, has provided evidence of the existence or execution of monopoly agreements (Lane, 2023).

## **5. Research Methodology**

As a solid framework for completely comprehending and comparing the implementation of competition laws in managing data, doctrinal research, which focuses on legal concepts and legislation, and case law research, which analyses court judgments, are both essential components. Within the context of China's and Pakistan's rapidly emerging digital economies, this research digs into the doctrinal and case law components of China's Competition Law and Pakistan's Competition Law in relation to data regulation.

### **5.1. Doctrinal Research**

An in-depth legal structure may be seen in China when one investigates the Anti-Monopoly Law (AML) and the Cyber Security Law. A fundamental aspect of doctrinal study is gaining a grasp of the important requirements that pertain to the localization of data, the transmission of data across international borders, and the protection of personal information. The Competition Act of 2010 and the Personal Data Protection Act, 2023 are two pieces of legislation that are being studied as part of Pakistan's doctrinal approach. An important part of the analysis is gaining knowledge of how these laws deal with issues such as data privacy, fair competition, and anti-competitive activities.

### **5.2. Case Law Research**

A better understanding of how Chinese courts interpret and apply competition rules to data-related concerns may be gained through the investigation of pertinent cases, such as those involving internet giants such as Alibaba and Tencent. This contributes to a better understanding of the gradually shifting judicial position. The analysis of competition cases and recent opinions issued by Pakistani courts may aid in assessing the actual implementation of competition rules in the digital arena. Specific instances relating to data protection aid in this understanding of legal precedents.

### **5.3. Comparative Analysis**

Examining the ways in which the theories of anti-money laundering and cyber security law match or diverge from the Competition Act and the Personal Data Protection Act, compare and contrast the legal underpinnings of each nation. Draw attention to the different legal frameworks' respective scopes and goals. Performing a side-by-side study of the particular requirements linked to data protection, including concerns such as permission, data localization, and cross-border data transfers, is an important step in the process of ensuring data protection. Examine the theological foundations that are responsible for establishing these guidelines. Case law relevant to the enforcement of competition rules in both countries should be evaluated as part of the enforcement mechanisms. It is important to identify notable instances that have had an impact on the enforcement environment and to investigate the role that regulatory agency like SAMR, CAC, and CCP play in the enforcement process.

### **5.4. Challenges and Implications**

Identifying issues within the legal doctrines of both nations, such as the need to strike a balance between encouraging innovation and prohibiting anti-competitive actions in the digital arena, is one example of potential doctrinal challenges. Discuss the ways in which landmark decisions have impacted the interpretation and implementation of competition rules in the context of data management. Case law implications in this context are discussed. It is important to investigate any changes or trends in judicial views.

### **5.5. Future Considerations**

Considering the progress that has been made in technology, it is important to discuss the possibility of adjustments or updates being required in the legal doctrines of both nations in order to manage the rising issues that are associated with the digital economy. In the process of developing case law, it is important to take into consideration how current and future cases may influence the landscape of competition law in relation to data management. Discuss the repercussions that this will have for companies and government authorities.

A comprehensive grasp of how China's and Pakistan's competition laws relate to data management in their fast-emerging digital economies may be obtained via a blend of doctrinal and case-law research approaches, as stated in the conclusion. In addition to shedding light on the existing legal environment, this research also offers insights into possible future changes and issues that may arise in this ever-changing regulatory atmosphere.

## **6. Comparative Analysis between Two Jurisdictions**

Competition rules have been created in China and Pakistan in order to govern data activities. Both countries are witnessing considerable development in their digital economies. In the context of China's fast-developing digital economy, the purpose of this research is to analyze and contrast the significance and efficiency of China's Competition Law with Pakistan's Competition Law in terms of data regulation.

### **6.1. Legislative Structures**

Both the Anti-Monopoly Law (AML) and the Cyber Security Law in China provide a comprehensive legal framework for the management of data and the competition that takes place in China. The principal piece of law in Pakistan is the Competition Act of 2010, while the most recent piece of legislation, the Personal Data Protection Act of 2022, tackles the issue of data protection.

### **6.2. Relevance to the Scope of Action**

In China, anti-money laundering (AML) has an extraterritorial reach, meaning that it affects both local and international organizations that operate in China. It places an emphasis on fair competition and prevents abuse of dominance. Despite the fact that it is

primarily concerned with avoiding anti-competitive behaviors, the Competition Act of Pakistan does not include any specific measures on data protection.

### 6.3. Provisions for the Protection of Data

The Cyber Security Law of China ensures that a safe digital environment is maintained by establishing criteria for the localization of data, the flow of data across international borders, and the protection of personal information. Pakistan's Personal Data Protection Act, which aligns with worldwide data protection standards, provides concepts of fair and legitimate processing, consent, and the rights of data subjects. These principles are intended to secure personal information.

### 6.4. Systems for Enforcing Compliance

China: The State Administration for Market Regulation (SAMR) and the Cyberspace Administration of China (CAC) are responsible for enforcing laws pertaining to competition and cyber security. They do this by conducting investigations and imposing fines to ensure compliance. The Competition Commission of Pakistan (CCP) is responsible for overseeing competition concerns in Pakistan; however, the efficiency of enforcement in the digital arena is developing as a result of the new data protection laws.

### 6.5. Implications for the World

**China:** China's data rules have an influence on worldwide enterprises, including digital giants such as Alibaba and Tencent. These policies raise worries about the national security of data and the fairness of competition on a global scale.

**Pakistan:** As Pakistan's digital economy continues to expand, the country's data security measures are becoming more and more significant for firms operating on a worldwide scale, which contributes to debates over cross-border data governance.

### 6.6. Obstacles and Things to Think About in the Future

**China:** Maintaining a healthy equilibrium between innovation and fair competition continues to be a problem, and improvements in technology that are ongoing may need legislation to be updated on a continuous basis. It is difficult to develop and enforce adequate data security measures in Pakistan due to the nature of the digital economy, which is constantly changing.

The conclusion is that China's Competition Law, in particular the Anti-Monopoly and Cyber Security Laws, plays a significant role in the process of influencing data practices inside the country's rapidly developing digital economy. On the other hand, Pakistan is starting to lay the groundwork for data regulation in its rapidly expanding digital ecosystem by enacting laws such as the Competition Act and the Personal Data Protection Act, which were only recently passed. Each nation is confronted with its own set of difficulties and possibilities, highlighting the need to maintain a state of continual adaptation to the ever-changing digital world.

## 7. Revising China's Competition Laws to Address the Challenges of the Digital Economy

In China's competitive rules and regulations, there was a lack of explicit mention or consideration given to data until a recent period. The parliamentarians and the State Administration for Market Regulation (SAMR) in China have recently made improvements to the competition legislation framework. These adjustments reflect a growing recognition of the significance and influence of data in the context of competition. The aim is to address various competitive challenges that have emerged in the digital economy.

In June 2022, amendments were made to the Anti-Money Laundering (AML) legislation with the aim of enhancing the regulation and oversight of digital platforms while

concurrently fostering their innovation and advancement. Businesses cannot use data, algorithms, technology, financial advantages, or platform regulations to engage in monopolistic activities under the Anti-Monopoly Law (AML). It also prohibits the unfair use of data, algorithms, technology, financial advantages, and platform regulations by market leaders. In February 2021, the State Administration for Market Regulation (SAMR) adopted its Anti-Monopoly Guidelines on the Platform Economy to regulate digital platforms, explicitly acknowledging the significance of facts in relation to abusive practices by dominant entities, mergers, and agreements that lead to monopolistic behavior (Gutkowski, 2023).

When assessing the extent of market dominance held by a platform, the SAMR (State Administration for Market Regulation) takes into account the platform's technological circumstances, namely its capacity to acquire, control, and process data. Additionally, the SAMR regards data acquisition as a factor that can impede the entry of new competitors into the market. The SAMR evaluates a platform's data holdings when determining its critical facility status. Due to its dominant market position, the Guidelines state that a platform that collects non-essential user information or uses big data and algorithms to discriminate may have engaged in abusive practices. However, the State Administration for Market Regulation (SAMR) acknowledges that safeguarding data and transaction security can be a valid justification for such conduct.

Data are of significant importance in the evaluation of competitiveness and the implementation of corrective measures in the process of reviewing mergers. When evaluating the effects of a potential merger on competition, the SAMR (State Administration for Market Regulation) will take into account various factors. These include the business's capacity to obtain, manage, and manipulate data, as well as its control over data interfaces. The SAMR will admit that if the merger gives the corporation the opportunity and desire to misuse customer data, it may lead to detrimental consequences for consumer interests. The potential conditions for merger imposed by the State Administration for Market Regulation (SAMR) may encompass the stipulation of divestiture or the provision of data access by the entities involved in the merger.

The Guidelines also acknowledge the potential of data to facilitate parties in reaching and executing monopolistic agreements, imposing unfair trade conditions, and coordinating conduct that violates the AML (Wu & Philipsen, 2023).

The 2017 AUCL amendment included an article to address online unfair competition practices. The State Administration for Market Regulation (SAMR) is now in the process of considering the adoption of legislation that is expressly designed to counter unfair competition practices within the internet sector, as outlined in the Anti-Unfair Competition Law (AUCL). The August 2021 draft of the proposed unfair competition legislation contains explicit mentions of data-related concerns. Business entities will be forbidden from utilizing data, algorithms, and other technical procedures to manipulate online traffic or manipulate user decisions, thereby impeding or disrupting other firms' legal online sales. They also cannot illegally obtain or exploit other firms' data, undermine their users' data security, or use data, algorithms, and other technical means to collect and analyze information about their counterparts to impose discriminatory trade conditions (Yin et al., 2023).

## **8. The impact of Data Regulation on Competition Law Enforcement**

While the data governance rules in China serve as the primary regulations governing data, it is worth noting that there are additional laws that can potentially exert regulatory control over data. As stated above, China's competition regulations are being revised to handle data concerns. Data governance regulations are new, notably the 2021 Data Security and Personal Information Protection regulations. As the legal framework for data governance becomes more intricate and all-encompassing, regulators gain familiarity with and authority over enforcing these laws. Consequently, the number of cases brought under these regulations increases. This trend suggests that data regulation will increasingly intersect and engage with various other laws, including competition laws. This phenomenon prompts inquiries on the interplay between data governance and other domains of regulation. In instances where data and data practices are subject to both data governance rules and competition laws, it is crucial to determine whether both sets of laws will be

imposed concurrently or if one set of rules or regulator will take precedence over the other. In the event of friction or inconsistency arising between competition rules and data governance regulations, potential avenues for resolution can be explored. How much will data governance impact the application and results of competition laws, and how will competition laws affect the data governance regime?

This section delves into the correlation between data regulation and competition law and its impact on the utilization of competition law for data regulation in China. It accomplishes this by taking into account two fundamental inquiries. The inquiry pertains to the circumstances in which it may be more appropriate and significant to enforce China's competition laws in order to tackle data-related concerns, either in conjunction with or instead of data governance regulations. Furthermore, it is worth considering the potential impact of data governance principles and outcomes on the enforcement and consequences of competition law (Zhao, Zhang, Sadiq, Hieu, & Ngo, 2023).

This inquiry will delve into the multifaceted interests, concerns, and objectives of consumers, businesses, and governmental entities that arise at the nexus of competition and data regulation. These threads possess the ability to extend and connect the two realms of regulation. Similar to the regulation of data, the state assumes the role of coordinating and mediating diverse interests and objectives through competition legislation. It serves as the final authority in determining which aims and interests should be prioritized and the manner in which they should be pursued. The explicit goals of the AML (Anti-Monopoly Law) and AUCL (Anti-Unfair Competition Law) encompass the prevention and prohibition of monopolistic and unfair competition practices. These laws protect consumer, business, and public interests as well as fair competition. Additionally, they aim to boost economic efficiency and preserve socialist market economy growth. Monopolies and chaotic competition hurt markets, customers, and economic growth. Competition law is seen as a way to regulate markets and an economic policy tool to help the state manage and coordinate state-market interaction. Gaining a comprehensive understanding of the coordination, balance, and prioritization of concerns, aims, and objectives within and between the two regulatory domains can yield useful insights into the state's strategy for effectively managing the challenges that arise at the convergence of competition law and data regulation. Furthermore, this topic also highlights the participants, political economy, and political and social issues that may affect the prioritizing and pursuit of various concerns, objectives, and interests (Han et al., 2024).

This approach aligns with China's overarching perspective on data regulation. Differential levels and types of regulatory attention are directed towards various data sets within the Chinese context. The classification of data, such as economic, individual, or national assets, or as possible hazards to state security or the public interest, will have an impact on the regulation of such data, determining the manner and extent of its governance. As previously said in Part I, data governance rules entail the classification of data according to their significance in fostering economic and social progress, as well as their potential impact on national security, public welfare, and the claims of people and entities. Moreover, information pertaining to national safety, which serves as the foundation of the national economy, crucial elements of individuals' well-being, and significant public concerns are considered the fundamental data of the state. Therefore, by actively considering the goals, issues, and preferences of consumers, businesses, and the government associated with data, it becomes possible to ascertain the appropriate classification of such data. This classification thereafter has a direct impact on the regulations and management strategies employed for handling the data. Certain categories of data are subject to more stringent safeguards, enhanced supervision, and regulatory measures compared to others. The regulation of such data may be carried out using various legal and policy frameworks, which may encompass competition laws as well (Miglionico, 2023).

## **9. Applicability of Competition Law To Data Regulation At The Intersection**

National and public security issues, like those in other countries, are extremely delicate politically and are of utmost importance to China. In cases where there are

legitimate competition concerns regarding data collection, utilization, or sharing practices. Competition issues are likely to take a back seat to national and public security considerations. Due to safety concerns, data will be categorized and restricted. The Cyber Security Law and Data Security Law acknowledge the danger unprotected data poses to national and public security and provide the government with the means to address these concerns and accomplish the desired results. In contrast, competition laws do not possess such direct provisions. In situations where data and behavior have implications for national and public security concerns and interests, it is probable that data governance rules will be prioritized over, and maybe even superseded, competition laws in order to directly regulate and resolve concerns relating to data. When competition concerns combine with industrial strategy, growth in the economy and society, and privacy issues, China's competition rules may play a larger role in data regulation. Chinese competition authorities frequently employ competition laws to address a range of challenges, in addition to traditional objectives such as economic efficiency, the welfare of customers, and safeguarding competition. Numerous historical instances have encompassed the behavior of corporations operating in sectors of significant industrial policy relevance or those involved in the provision of vital services and products to the general public. In the analysis of competition law, adherence to legal statutes and regulations, particularly those specific to the respective sectors, has been duly taken into account. Moreover, as discussed above, the consideration of data protection has played a significant role in the decision-making processes of Chinese courts and competition agencies in relation to competition laws. The aforementioned enforcement experience indicates that competition law may serve as a viable means to address the aforementioned combination of interests, concerns, and objectives, regardless of the application of data governance legislation (Parker, 2020).

The dynamics between the State Administration for Market Regulation (SAMR) and the various state entities vested with authority to execute data governance legislation will also have an impact on the process of evaluating interests, concerns, and objectives pertaining to data and the potential application of competition law to control such data in specific situations. The presence of numerous regulatory bodies might potentially lead to bureaucratic turf battles and the emergence of conflicting interests and objectives. Factors like their respective political influence and significance have an impact on the dynamics between the SAMR and state authorities in charge of data rules and guidelines, namely the CAC, MIIT, MPS, and MSS. Additionally, the political sensitivity of the relevant data and behavior, as well as the state's desired message to external entities, all influence these interactions and relationships. The China Administration of Cyberspace (CAC) is a regulatory agency that was founded in 2014 with the primary objective of overseeing online content. It functions as a government institution and operates directly under the Central Committee of the Chinese Communist Party (CCP). Despite encountering political and bureaucratic opposition from other state authorities reluctant to cede regulatory control, the CAC has experienced a recent increase in political influence due to the expansion of its regulatory jurisdiction and the implementation of more prominent initiatives. The Ministry of State Security (MSS), Ministry of Public Security (MPS), and Ministry of Industry and Information Technology (MIIT) hold significant political influence in China due to their extensive mandates and historical significance. As a result, these state entities are regarded as some of the most politically influential bodies in the country. In order to further their own interests, these additional regulatory bodies possess the ability to independently initiate enforcement measures in accordance with data governance legislation. Consequently, they may actively contest, intervene in, or exert influence over competition law activities undertaken by the State Administration for Market Regulation (SAMR) that exhibit areas of overlap with their own jurisdiction (Hazlett, Ramos, & Smith, 2023).

State engagement in competition law investigations and disputes is not new. Tencent's incompatible instant messaging software with Qihoo 360's antivirus and privacy protection software led the Ministry of Industry and Information Technology (MIIT) to criticize both companies. Thus, the MIIT ordered public apologies and collaboration, which the corporations followed despite competition law actions. It is well known that MIIT strongly opposed the competition regulator's inquiry into China Telecom and China Unicom's misuse of dominance. Instead of financial fines, commitments were used to resolve competitive problems due to this objection. Despite its increased capabilities compared to previous authorities, the SAMR remains a relatively recent government entity that is now navigating its interactions with other state agencies and delineating the limits of their



separate regulatory jurisdictions. However, the regulatory and enforcement campaign that commenced in 2020 has led to a noticeable enhancement in the SAMR and competition law authority, particularly in relation to internet and technology businesses.

The State Administration for Market Regulation (SAMR) demonstrated prompt and decisive measures in addressing the postponement of the Ant Group's initial public offering in November 2020. In a short span of time, the State Administration for Market Regulation (SAMR) promptly issued a preliminary version of the Anti-Money Laundering (AML) guidelines, which are intended to be applicable to digital platforms. Additionally, the SAMR collaborated with other regulatory bodies to convene an administrative guidance meeting, which garnered participation from 27 prominent digital platforms in China. Furthermore, the SAMR initiated two separate investigations into prior merger activities conducted by Alibaba and Tencent. A prominent antitrust inquiry was initiated by the regulatory body, focusing on Alibaba, in December 2020. This investigation was regarded as a subject of significant national political importance. Additionally, the regulatory authorities fined Alibaba and Tencent the most for failing to notify the competition authority of their past mergers, thereby bypassing the anti-monopoly review process. The implementation of these prompt and crucial measures would have facilitated the SAMR's effectively positioning itself as a proactive and efficient regulatory body in the eyes of China's key decision-makers, other regulatory entities, state authorities, businesses, and the general public. Additionally, it would have showcased the regulatory efficacy and significance of the AML as a regulatory tool (Srivastava et al., 2023).

Subsequently, the SAMR has emerged as a prominent and proactive regulatory authority, primarily employing its competition law jurisdiction in its endeavors to address and regulate internet and technology firms. The regulatory authority has levied a substantial penalty exceeding RMB18.2 billion on Alibaba for engaging in market dominance abuse. Meituan has also been fined for similar dominance abuse, while reports indicate that an antitrust investigation into Didi Chuxing has been initiated. Furthermore, the authority has prohibited the merger of two prominent Chinese digital platforms specializing in video game live streaming. Additionally, various internet and technology companies have faced penalties for failing to report their previous mergers for anti-monopoly review.

The Chinese government's top brass supports SAMR's work. China has stressed competition legislation in its regulation of the internet and technology industries. It has advocated for competition law reform, regulator action against monopolies, fair competition, and antitrust supervision. The State Administration for Market Regulation now has more enforcement power under China's updated AML law. For instance, the SAMR (State Administration for Market Regulation) may investigate mergers that do not fulfill obligatory notice requirements but might eliminate or limit competition. The regulatory authority has also increased administrative fines for anti-monopoly law infractions. To improve competition in law enforcement, institutions have been changed. The State Administration for Market Regulation (SAMR) promoted the AML bureau to deputy ministerial in November 2021. This institution became the State Anti-Monopoly Bureau under the SAMR deputy minister. Additionally, the bureau's manpower will be expanded. Increased legal, institutional, and political authority of the SAMR and the recently passed digital economy competition law legislation will help it enforce its competition law responsibilities in the internet and technology industry, including data regulation and dispute resolution with other regulatory bodies (Mungan & Yun, 2023).

With that being stated, the primary concern of the state is to impose stricter regulations on internet and technology corporations, which has broadened the jurisdiction for all regulatory bodies to initiate measures against such entities, particularly digital platforms. Like previous campaigns, this regulatory and enforcement strategy sought to remove political and logistical barriers that may have sheltered internet and technology businesses from regulation. It has also encouraged and empowered governmental entities to regulate the internet and technology industries.

The China Advertising Association (CAC), similar to the State Administration of Market Regulation (SAMR), has demonstrated significant activity and prominence in the campaign, augmenting its monitoring authority and acquiring political influence as a

consequence. As an illustration, the regulatory body initiated cyber security assessments on multiple companies that had just undergone initial public offerings on American stock exchanges, citing apprehensions related to national security, safeguarding of data, and protection of personal information. The cyber security assessment conducted on Didi Chuxing, the prominent ride-hailing company in China, led to the imposition of a penalty amounting to RMB 8.026 billion. The China Administration of Cyberspace (CAC) issued orders to numerous applications, instructing them to address their unlawful practices of gathering and utilizing personal data. Additionally, the CAC imposed fines on certain internet corporations for violating the Cyber security Law by disseminating information in contravention of its provisions.

As with prior enforcement operations, the SAMR (State Administration for Market Regulation) and CAC (Cyberspace Administration of China) have been key players in this one. Throughout this effort, regulators and other state agencies have coordinated and collaborated on certain activities. The State Administration of Taxation, SAMR, Ministry of Natural Resources, Ministry of Transportation, CAC, and Ministry of Public Safety and Security reviewed Didi Chuxing's cyber security. The SAMR, CAC, and State Administration for Taxation ordered 34 key Chinese internet platforms to self-examine and correct misbehavior. CAC, MIIT, MPS, and SAMR also campaigned for three months to outlaw spy cameras and hidden-camera movies. States have worked together to regulate the internet and technology industries. These include restricting mobile app data collection, regulating algorithmic recommendations by internet and technology companies, protecting automotive data, and protecting ride-hailing and food delivery drivers. Despite the varied variety of regulators and state authorities participating in the enforcement campaign and the problems they addressed, it seems that others did not resist their attempts to establish, protect, and perhaps expand their regulatory powers (Roberts, 2023).

As of the present moment, the government of China has indicated its intention to reduce the level of regulatory measures pertaining to internet and technology enterprises within China. Nevertheless, it is important to note that the diminished intensity of enforcement measures directed towards specific enterprises does not mean a reversion to the lenient regulatory landscape that internet and technology companies in China had previously experienced. The activities of the concerned entities have been subjected to enhanced and comprehensive regulation through the recent adoption of legal and regulatory measures during the campaign. Furthermore, additional regulations will be necessary to ensure the continued implementation of data governance laws, accompanied by intensified enforcement efforts in this regard.

In addition, it is noteworthy that the campaign not only enhanced the political and implementation capabilities of the CAC and SAMR but also bestowed upon these two regulatory bodies an augmented authority to oversee and govern internet and technology enterprises. The enhancements implemented in the authorized and organized structure pertaining to competition law, along with the bolstering of the SAMR's authority, would facilitate the enforcement of China's competition laws by effectively addressing data-related competition concerns. Hence, despite the increasing implementation of data governance legislation by various regulatory bodies and the possibility of encountering bureaucratic and regulatory disputes and challenges, China's competition laws may be used more for data control (Tallberg et al., 2023).

## **10. The Possible Impact of Data Governance Considerations on the Enforcement of Competition Law**

Data governance goals, interests, and concerns must be considered when applying competition law to data and data practices. These factors, which are rarely related to competition, are expected to influence competition law decisions. As shown in Part II, the current framework of competition law, along with how the AUCL and AML are interpreted and used by courts and regulators, makes it possible to look at specific cases where data security and privacy are important. Moreover, the SAMR (State Administration for Market Regulation) issued preliminary recommendations in October 2021, aiming to categorize digital platforms and delineate their corresponding obligations. The draft guidelines demand digital platforms follow anti-monopoly, unfair competition, and consumer protection measures. The rules also outline digital platforms' cyber security, data security, privacy,

workers' rights, environmental preservation, and tax duties. Most of these concerns fall outside the SAMR's market regulation jurisdiction. While guidelines lack legal enforceability, they serve to delineate the SAMR's intended course of action in fulfilling its responsibilities and implementing regulations pertaining to digital platforms. The draft guidelines propose that the SAMR (State Administration for Market Regulation) adopt a comprehensive strategy for regulating digital platforms. This approach may encompass factors beyond competition and consumer considerations, thereby influencing the implementation of competition laws (Zhao et al., 2023)

China's mandated consultation procedure for bureaucratic decision-making may help integrate data governance concepts, concerns, and goals into competition legislation. The State Administration for Market Regulation (SAMR) consults with relevant state authorities when adopting AML or AUCL procedures. These consultations are used to get their feedback on an issue and their approval of the final decision. The State Administration for Market Regulation (SAMR) often consults the China Anti-Monopoly Committee (CAC) and the Ministry of Industry and Information Technology (MIIT) when investigating internet and technology mergers. During the consultation process, other state agencies might voice their concerns and influence competition law decisions. Historical instances have been documented wherein the involvement of other state authorities seems to exert an influence on decision-making processes pertaining to the Anti-Money Laundering (AML) framework and its implementation. In certain instances, it appears that certain merger remedies were primarily focused on addressing the concerns expressed by engaged government departments rather than specifically targeting the potential anticompetitive impacts. The opacity of China's administrative decision-making and governance structure poses challenges in understanding the process, participants, and mechanisms for balancing and coordinating diverse topics (Knapstad, Naterstad, & Bogen, 2023).

While it is true that data governance can play a role in the decision-making process of competition legislation, it should be noted that the presence of data governance does not guarantee that competition concerns will be adequately evaluated, nor does it imply that they will be missed or disregarded. The State Administration for Market Regulation (SAMR) is required to fulfill its obligations and duties as the regulatory body for competition. Both the SAMR and the courts must ascertain the appropriate approach to addressing anti-monopoly or unfair competition practices in accordance with competition law principles. The existing analytical frameworks and competition law norms place restrictions on the ability to manage data governance-related interests, concerns, and goals within the purview of China's competition legislation.

The prevalence of competition law decisions in the published literature demonstrates a clear adherence to established competition law terminology and analytical frameworks. The AML verdicts generally align with international competition law rules and are consistent with the approaches used by other jurisdictions. This phenomenon has been observed even in instances where it appears that factors unrelated to competition did have an impact on the results. Indeed, the inclusion of non-competition variables in AML decisions was generally uncommon, even if they were permitted to be taken into account within the framework of the AML. These rulings illustrate that competition regulators and courts in China have been aware of the need to support their conclusions using a competition law analytical framework. Simultaneously, the aforementioned phenomenon has obscured the examination and impact of non-competition elements in the process of decision-making within the realm of competition law, giving rise to concerns over transparency. The inclusion of non-competition variables, including data governance-related problems, in the considerations and resolutions of the State Administration for Market Regulation (SAMR) and the Chinese courts within the framework of competition law introduces complexities that hinder comprehension of the specific timing and methods by which these factors will be taken into account and dealt with (Funta & Ondria, 2023).

## **11. Policy Recommendations for Pakistan**

As a keystone in the process of regulating and strengthening the economic market, Pakistan's competition legislation plays a crucial role in figuring out how to navigate the complexity of the quickly growing digital economy.

The competition law takes on the role of a vital instrument in the ever-changing environment of the digital economy, which is characterized by ongoing innovation and business models that are disruptive. The prevention of monopolistic behaviors, which have the potential to inhibit innovation and limit competition, is the principal duty of this authority. A piece of legislation that helps to preserve a fair and open market structure is one that encourages an environment in which enterprises compete on the basis of their merit (Zhang & Qu, 2024).

The function that competition law plays in protecting the interests of consumers is one of the most important aspects of this area of law. This legal framework serves as a barrier against exploitative behaviors in the digital sphere, which is filled with concerns about the privacy of users' data and the protection of users. When it comes to maintaining consumer welfare, it becomes an essential component since it guarantees a wide range of options and value for customers. Competition law's impact on stimulating innovation and providing support for startups is another way in which its significance is highlighted. Additionally, it fosters a culture of entrepreneurship and inventiveness within the digital environment by prohibiting practices that are anti-competitive. This opens the door for new market entrants.

One of the most important aspects related to global competitiveness is the role that competition law plays. The digital economy is expanding beyond national lines, and Pakistan's place in the international arena is being strengthened by the establishment of a solid legal framework. The country is positioned as a competitive actor in the global digital arena when it complies with competition legislation, which instills trust in foreign investors and streamlines the process of cross-border partnerships (Jia, Rusinek, Xiao, & Wood, 2021).

The convergence of competition law and data protection legislation becomes an absolute need in the setting of the digital economy, which is characterized by the fact that data is a valuable asset. This comprehensive strategy addresses data abuse concerns while also ensuring responsible management of private data and assisting in the development of a trustworthy digital ecosystem.

In order for competition laws to adapt to the fast changes that are occurring in the digital realm, adaptability is a crucial quality that they need to possess. It is necessary to have a legal framework that is adaptable in order to successfully handle new difficulties as technologies such as artificial intelligence and block chain continue to transform the economic environment.

Another essential component is the need for cooperation between the authority in charge of competition and other regulatory authorities. It is possible to establish a holistic approach to addressing challenges that are special to the digital economy by aligning efforts with institutions that supervise telecommunications and technology. This will result in legislation that is more thorough and accurate (Ju et al., 2024).

Within the context of the administration of the rapidly expanding digital economy, Pakistan's competition legislation appears as a cornerstone. In addition to fostering innovation and enhancing global competitiveness, its complex responsibilities include the promotion of fair competition, the protection of consumer interests, and the support of innovation. When it comes to guiding the digital economy towards continuous growth and development, it is vital to strike a careful balance between regulatory control and the cultivation of an environment that is beneficial to business (Dong et al., 2023).

In order to regulate the digital economy for the Pakistani market, Pakistani regulatory and legislative authorities need to draft a detailed study of the effective application of the Chinese competition law business model.

One of the most promising approaches to controlling the digital economy in the Pakistani market is the effective implementation of the business model based on Chinese competition legislation. It is possible for Pakistan to gain useful lessons from China's experience in using competition legislation to handle the complexities of the digital world.

The establishment of a regulatory framework that encourages fair competition and handles the specific issues given by the digital economy is something that Pakistan is able to do by adopting and modifying components of this model.

The Chinese competition law places a strong emphasis on the suppression of monopolistic behaviors, which helps to create an environment in which enterprises compete based on their inherent worth. This method is in line with the need to cultivate a market structure that is both open and fair in Pakistan's digital economy. Preventing the dominance of a small number of firms and supporting a landscape that is both diversified and competitive are the goals of this approach (Han et al., 2024).

While the Chinese model places a strong emphasis on consumer protection, Pakistani rules may benefit from adopting similar ideas in order to better protect the interests of consumers. When it comes to ensuring that customers have options and are compensated for their participation in the digital marketplace, it is of the utmost importance to address concerns such as data privacy and user protection.

Particularly pertinent to Pakistan's digital economy is the Chinese model's focus on fostering innovation and fostering the growth of startups. Establishing a culture of entrepreneurship and contributing to the development of creative solutions may be accomplished via the regulatory framework's ability to discourage anti-competitive activities, therefore paving the way for new entrants. As another area in which the Chinese model thrives, global competitiveness is particularly noteworthy. Pakistan's status in the global digital arena would be improved if it were to successfully execute a comparable method for the nation. In order to attract foreign investment and create prospects for cross-border collaborations and partnerships, it would be beneficial to align with international standards and current best practices (Staab, Zschech, & Krause-Rehberg, 2000).

It is essential for Pakistan's digital economy to have a synergy between competition legislation and data protection that is observed in China. In order to foster confidence in digital transactions and services, which is an essential component of a functioning digital economy, it is important to ensure that sensitive information is handled in a responsible manner. The Chinese model has a number of important characteristics, one of which is adaptability, which enables flexibility in reaction to the fast changes that are occurring in the digital world. Because of this flexibility, the regulatory framework is able to continue to be successful in tackling new difficulties that are brought about by technological improvement (Sukrat & Leeraphong, 2024).

A comprehensive approach to the regulation of the digital economy requires collaboration with a variety of regulatory organizations, as was clearly proven in China. It is possible to get a more thorough knowledge of the business by aligning efforts with bodies that govern technology and telecommunications. This will result in regulation that is more effective and coordinated.

For the purpose of regulating Pakistan's digital economy, the successful application of the Chinese competition law business model provides a convincing template that Pakistan may follow. It is possible for Pakistan to develop a strong regulatory framework that nurtures a digital ecosystem that is both sustainable and competitive if it incorporates essential concepts such as the prevention of monopolistic behaviors, the prioritization of consumer protection, the encouragement of innovation, and the guarantee of global competitiveness.

## **12. Conclusion**

In China, similar to several other nations globally, there is a growing recognition among individuals, organizations, and the government regarding the significance of data, as well as the potential benefits and drawbacks it entails. The growth of the internet, the electronic economy, and related techniques has further increased this awareness. The government of China adopts a comprehensive perspective when analyzing data, taking into account its political and security ramifications. It perceives data as valuable economic

assets, which can also have public repercussions, and acknowledges their potential to contribute to China's economic growth and developmental objectives. China is currently in the process of building a data governance regime that is becoming more advanced. This regime considers many different public and private goals, interests, and concerns. The government exercises regulatory authority over the access, utilization, and transmission of data while advancing the internet, the digital economy, and data and technology. This is done to help the state control relevant businesses, industries, and data. The recent campaign aimed at internet and technology businesses has underscored the significance of data regulation.

Data regulation in China is projected to increasingly rely on competition law. The State Administration for Market Regulation (SAMR) and private litigants can enforce China's competition law thanks to new rules for tech and internet companies, support for competition law enforcement from China's leaders, an updated competition law framework that addresses issues of unfair competition and anti-monopoly in the digital economy, and better institutions. These regulations target internet and technology corporations' data and data practices, notably digital platforms. The area where data regulation and competition law meet, along with the many players, goals, concerns, and interests that are involved, creates difficulties that are likely to limit how competition law works and is applied to data.

The interplay between legal frameworks goes beyond data and behavior. Political effect, stakeholder interconnectivity, data aims, concerns, and interests, and governance and political environment and dynamics shape this relationship. This article states that China's competition laws may control industrial policy, economic and social progress, privacy, and personal data. Data governance regulations may address national and public security issues better than competition legislation.

China is not alone in how varied interests, concerns, goals, and political variables affect data and competition regulation, regulatory frameworks, and enforcement. The global landscape is witnessing a shift in political sentiment towards internet and technology corporations, accompanied by a growing emphasis on the significance of competition law enforcement and reform in the ongoing discourse around the regulation of these entities. This trend is observable across numerous countries. The SAMR's focus on the internet and technology aligns with several other competition regulators. The state's interests, concerns, and goals in competition law, markets, and data governance reflect China's socialist political and legal framework and active state involvement in the market, economy, and society.

#### **Authors Contribution:**

Shahzada Aamir Mushtaq: Conceived the idea and designed the analysis; Analyzed and interpreted the data; Contributed analysis tools or data; Wrote the paper, Manuscript Draft.  
Khurram Baig: Proofread, Review and Designed the analysis; Manuscript Draft.  
Saifullah Hassan: Proofread, Review and Designed the analysis; Manuscript Draft  
Waqas Ahmad: Proofread, Review and Designed the analysis; Manuscript Draft

#### **Conflict of Interests/Disclosures**

The authors declared no potential conflicts of interest w.r.t the research, authorship and/or publication of this article.

#### **References**

- Abada, I., & Lambin, X. (2023). Artificial intelligence: Can seemingly collusive outcomes be avoided? *Management Science*. doi:<https://doi.org/10.1287/mnsc.2022.4623>
- Bergqvist, C., & Choi, Y. S. (2023). Controlling market power in the digital economy: The EU and Asian approaches. *Computer Law & Security Review*, 50, 105834. doi:<https://doi.org/10.1016/j.clsr.2023.105834>
- Bourguignon, L., Faivre, J.-P., & Turq, A. (2004). Ramification des chaînes opératoires: une spécificité du Moustérien. *Paléo*, 16, 37-48.
- Bui, T. N., Nguyen, X. H., & Pham, K. T. (2023). The effect of capital structure on firm value: A study of companies listed on the Vietnamese stock market. *International Journal of Financial Studies*, 11(3), 100. doi:<https://doi.org/10.3390/ijfs11030100>
- Caglar, A. E., Daştan, M., & Rej, S. (2024). A new look at China's environmental quality: how does environmental sustainability respond to the asymmetrical behavior of the

- competitive industrial sector? *International Journal of Sustainable Development & World Ecology*, 31(1), 16-28. doi:<https://doi.org/10.1080/13504509.2023.2248584>
- Caliskan, H., Açikkalp, E., Rostamnejad Takleh, H., & Zare, V. (2023). Advanced, extended and combined extended-advanced exergy analyses of a novel geothermal powered combined cooling, heating and power (CCHP) system. *Renewable Energy*, 206, 125-134. doi:<https://doi.org/10.1016/j.renene.2023.02.032>
- Colangelo, M., Korzh, B., Allmaras, J. P., Beyer, A. D., Mueller, A. S., Briggs, R. M., . . . McCaughan, A. N. (2023). Impedance-matched differential superconducting nanowire detectors. *Physical Review Applied*, 19(4), 044093. doi:<https://doi.org/10.1103/PhysRevApplied.19.044093>
- Djalilova, Z. (2023). PEDAGOGICAL EDUCATIONAL TECHNOLOGY: ESSENCE, CHARACTERISTICS AND EFFICIENCY. *Академические исследования в современной науке*, 2(23), 29-38. doi:<http://www.econferences.ru/index.php/arims/article/view/8999>
- Dong, D., Wang, T., Sun, Y., Fan, J., & Lu, Y.-C. (2023). Hydrotropic solubilization of zinc acetates for sustainable aqueous battery electrolytes. *Nature Sustainability*, 6(11), 1474-1484. doi:<https://doi.org/10.1038/s41893-023-01172-y>
- Edwards, E. C., Holcombe, A., Brown, S., Ransley, E., Hann, M., & Greaves, D. (2023). Evolution of floating offshore wind platforms: A review of at-sea devices. *Renewable and Sustainable Energy Reviews*, 183, 113416. doi:<https://doi.org/10.1016/j.rser.2023.113416>
- Ezrachi, A., & Stucke, M. E. (2023). The Darker Sides of Digital Platform Innovation. *Wirtschaft und Wettbewerb*(8).
- Funta, R. (2012). Abuse of dominant position in EU and US Law. doi:<http://hdl.handle.net/20.500.11956/47516>
- Funta, R., & Ondria, P. (2023). Threats to Diversity of Opinion and Freedom of Expression via Social Media. *TalTech Journal of European Studies*, 13(2), 29-45. doi:<https://doi.org/10.2478/bjes-2023-0014>
- Garces, E., & Colangelo, G. (2023). Markets, Competition, and Fairness in the EU. doi:<https://dx.doi.org/10.2139/ssrn.4349587>
- Gauri, V., Rahman, T., & Sen, I. K. (2023). Shifting social norms to reduce open defecation in rural India. *Behavioural Public Policy*, 7(2), 266-290. doi:<https://doi.org/10.1017/bpp.2020.46>
- Glass, V., & Tardiff, T. (2023). Analyzing Competition in the Online Economy. *The Antitrust Bulletin*, 68(2), 167-190. doi:<https://doi.org/10.1177/0003603X231163001>
- Goode, J. (2021). *The Science of Wine: From Vine to Glass-3rd Edition*: Univ of California Press.
- Gutkowski, B. (2023). Consumer Welfare of the Future: Harm to Innovation as an Antitrust Injury. *San Diego L. Rev.*, 60, 223.
- Han, W., Wu, S., Dong, F., Han, W., Chu, Y., Su, L., & Tang, Z. (2024). A confined growth strategy to construct 3DOM SiO<sub>2</sub> nanoreactor in-situ embedded Co<sub>3</sub>O<sub>4</sub> nanoparticles catalyst for the catalytic combustion of VOCs: Superior H<sub>2</sub>O and SO<sub>2</sub> resistance. *Nano Research*, 17(1), 207-220. doi:<https://doi.org/10.1007/s12274-023-5498-0>
- Hazlett, C., Ramos, A. P., & Smith, S. (2023). Better individual-level risk models can improve the targeting and life-saving potential of early-mortality interventions. *Scientific Reports*, 13(1), 21706. doi:<https://doi.org/10.1038/s41598-023-48888-7>
- Jia, B., Rusinek, A., Xiao, X., & Wood, P. (2021). Simple shear behavior of 2024-T351 aluminum alloy over a wide range of strain rates and temperatures: Experiments and constitutive modeling. *International Journal of Impact Engineering*, 156, 103972. doi:<https://doi.org/10.1016/j.ijimpeng.2021.103972>
- Ju, W., Fang, Z., Gu, Y., Liu, Z., Long, Q., Qiao, Z., . . . Zhang, M. (2024). A comprehensive survey on deep graph representation learning. *Neural Networks*, 106207. doi:<https://doi.org/10.1016/j.neunet.2024.106207>
- Khan, A. S., & Liu, H. (2012). A new approach for ductile fracture prediction on Al 2024-T351 alloy. *International Journal of Plasticity*, 35, 1-12. doi:<https://doi.org/10.1016/j.ijplas.2012.01.003>
- Knapstad, M. K., Naterstad, I., & Bogen, B. (2023). The association between cognitive impairment, gait speed, and Walk ratio. *Frontiers in Aging Neuroscience*, 15, 1092990. doi:<https://doi.org/10.3389/fnagi.2023.1092990>
- Kölbel, M. (2023). Varieties of conceptual analysis. *Analytic Philosophy*, 64(1), 20-38. doi:<https://doi.org/10.1111/phib.12249>



- Lane, T. J. (2023). Protein structure prediction has reached the single-structure frontier. *Nature Methods*, 20(2), 170-173. doi:<https://doi.org/10.1038/s41592-022-01760-4>
- Li, W., Wang, C.-h., Cheng, G., & Song, Q. (2023). International conference on machine learning. *Transactions on machine learning research*.
- Liu, M., Zheng, R., Li, J., & Ma, C. (2020). Achieving ultrahigh tensile strength of 1 GPa in a hierarchical nanostructured 2024 Al alloy. *Materials Science and Engineering: A*, 788, 139576. doi:<https://doi.org/10.1016/j.msea.2020.139576>
- Migliorico, A. (2023). Regulating Innovation through Digital Platforms: The Sandbox Tool. *European Company and Financial Law Review*, 19(5), 828-853. doi:<https://doi.org/10.1515/ecfr-2022-0029>
- Mungan, M. C., & Yun, J. M. (2023). A Reputational View of Antitrust's Consumer Welfare Standard. *George Mason Law & Economics Research Paper*(23-05).
- Parker, L. D. (2020). The COVID-19 office in transition: cost, efficiency and the social responsibility business case. *Accounting, Auditing & Accountability Journal*, 33(8), 1943-1967. doi:<https://doi.org/10.1108/AAAJ-06-2020-4609>
- Roberts, I. (2023). *Satow's diplomatic practice*: Oxford University Press.
- Schneider, F., Kamal, O., Jin, Z., & Schölkopf, B. (2023). Mo<sup>^</sup> usai: Text-to-music generation with long-context latent diffusion. *arXiv preprint arXiv:2301.11757*. doi:<https://doi.org/10.48550/arXiv.2301.11757>
- Singh, I., Blukis, V., Mousavian, A., Goyal, A., Xu, D., Tremblay, J., . . . Garg, A. (2023). *Progprompt: Generating situated robot task plans using large language models*. Paper presented at the 2023 IEEE International Conference on Robotics and Automation (ICRA).
- Spulber, D. F. (2023). Antitrust and innovation competition. *Journal of Antitrust Enforcement*, 11(1), 5-50. doi:<https://doi.org/10.1093/jaenfo/jnac013>
- Srivastava, S., Ranjan, S., Yadav, L., Sharma, T., Choudhary, S., Agarwal, D., . . . Garg, A. (2023). Advanced spectroscopic techniques for characterizing defects in perovskite solar cells. *Communications Materials*, 4(1), 52. doi:<https://doi.org/10.1038/s43246-023-00379-y>
- Staab, T., Zschech, E., & Krause-Rehberg, R. (2000). Positron lifetime measurements for characterization of nano-structural changes in the age hardenable AlCuMg 2024 alloy. *Journal of materials science*, 35, 4667-4672. doi:<https://doi.org/10.1023/A:1004838619943>
- Sukrat, S., & Leeraphong, A. (2024). A digital business transformation maturity model for micro enterprises in developing countries. *Global Business and Organizational Excellence*, 43(2), 149-175. doi:<https://doi.org/10.1002/joe.22230>
- Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research. *arXiv preprint arXiv:2305.11528*. doi:<https://doi.org/10.48550/arXiv.2305.11528>
- Wach, K., Duong, C. D., Ejdys, J., Kazlauskaitė, R., Korzynski, P., Mazurek, G., . . . Ziemba, E. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. *Entrepreneurial Business and Economics Review*, 11(2), 7-30. doi:<https://www.ceeol.com/search/article-detail?id=1205845>
- Wang, W., Chen, Z., Chen, X., Wu, J., Zhu, X., Zeng, G., . . . Qiao, Y. (2024). VisionLlm: Large language model is also an open-ended decoder for vision-centric tasks. *Advances in Neural Information Processing Systems*, 36.
- Wendy Hodsdon, N., & Zwickey, H. (2010). NMJ Original Research: Reproducibility and Reliability of Two Food Allergy Testing Methods.
- Wu, Q., & Philipsen, N. J. (2023). The law and economics of tying in digital platforms: comparing tencent and android. *Journal of Competition Law & Economics*, 19(1), 103-122. doi:<https://doi.org/10.1093/joclec/nhac011>
- Yin, H., Zhang, W., Zhu, L., Meng, F., Liu, J., & Wen, G. (2023). Review on lattice structures for energy absorption properties. *Composite Structures*, 304, 116397. doi:<https://doi.org/10.1016/j.compstruct.2022.116397>
- Zhang, Y., & Qu, Y. (2024). Has the digital economy improved the consumption of poor and subsistence households? *China Economic Review*, 83, 102083. doi:<https://doi.org/10.1016/j.chieco.2023.102083>
- Zhao, L., Zhang, Y., Sadiq, M., Hieu, V. M., & Ngo, T. Q. (2023). Testing green fiscal policies for green investment, innovation and green productivity amid the COVID-19 era. *Economic Change and Restructuring*, 56(5), 2943-2964. doi:<https://doi.org/10.1007/s10644-021-09367-z>



Zhi, Z., Li, H., Geurs, I., Lewille, B., Liu, R., Van der Meeren, P., . . . van Bockstaele, F. (2024). Dual stabilization of O/W/O double emulsions by proteins: An interfacial perspective. *Food Hydrocolloids*, 148, 109488.  
doi:<https://doi.org/10.1016/j.foodhyd.2023.109488>