Business Barriers and Big Data in India And Africa: Protection of Personal Information Act (Popia) And Competition Law

Sai Datta Vamshi
BBA LLB, VI Semester, ABBS School of Law, Bangalore, Affiliated to Karnataka State Law University
Khachitri T.N
BBA LLB, IV Semester, ABBS School of Law, Bangalore, Affiliated to Karnataka State Law University
Prof.Arathy,K.B.
Principal, ABBS School of Law, Bangalore, Affiliated to Karnataka State Law University
Dr.Devaraja Nayaka, K.M.
Associate Professor, Department of Commerce and Management, Acharya Bangalore B-School, Affiliated to Bangalore University, Bengaluru, Karnataka, India.

ABSTRACT

Big Data has quickly penetrated most business areas in the past decade, posing challenges for the effectiveness of existing data protection rules, on one hand, but also for different aspects of competition law and its enforcement, on the other hand. Access to customer contact data or customer preferences has impacted on competitive parameters, raising completely new questions of competition law, e.g. in the context of data portability or digital cartels. However, the more fundamental issue arises if and how data protection compliance can or should be a parameter in the assessment of competition authorities around the world, being a well-known fact that, in principle, competitive assessment is bound only by welfare considerations.

Personal data has multiple impacts on all pillars of competition law – anti competitive agreements, abuse of dominance and merger control. While abuse of dominance and merger control relate to competitive harm via the access to greater customer data, the classic price fixing cartels are being replaced by seemingly irretraceable, big data-based price fixing algorithms. We shall be covering the aspects of the Data Protection in the light of Competition law covering the interest in merger review, fundamental right of data protection and the abuse of dominance along with the legal frameworks covering the aspects under the African law.

Keywords: *Big Data, data protection, privacy issue, Indian Competition Act, African law*

Introduction

The Indian competition law regime has grown considerably in the last six years ever since the Act became operational in 2009. Prior to the operationalization of the Competition Act in May 2009, MRTP Act was the operational law that regulated certain aspects of competition.

Big data' has been described as a voluminous amount of data which is mined by business entities for commercial gain and other purposes. Big data has been characterized by the four V's: the *volume* of data; the *velocity* at which data is collected, used, and disseminated; the *variety* of the information aggregated; and finally the *value* of the data. After collection of such data, what comes into picture is 'big analytics', a term referring to the complex process of examination of big data using specialised algorithms to uncover hidden patterns, extracting useful information such as consumer preferences, market trends, etc. Such information helps business entities plan their future business policies.

Review of Literature

The emergence of big data as an asset for market players does not only raise data protection issues but also leads to competition considerations. The rapid growth of data application in this digitized economy unveils the scope of data protection in the realm of competition law. However, at the same time, it should be noted that competition and data protection law are two different legal regimes having different causes of

concern. This implies that pure data protection issues should be considered by data protection authorities.

According to Russom (2011) the term "Big Data" has been applied to datasets that grow so large that they become awkward to work with using traditional database management systems. They are data sets whose size is beyond the ability of commonly used software tools and storage systems to capture, store, manage, as well as process the data within a tolerable elapsed time. Hence, big data analytics is where advanced analytic techniques are applied on big data sets. Analytics based on large data samples reveals and leverages business change. However, the larger the set of data, the more difficult it becomes to manage Russom (2011).

EMC (2012) study defined that the big data is data whose scale, distribution, diversity, and/or timeliness require the use of new technical architectures, analytics, and tools in order to enable insights that unlock new sources of business value. Three main features characterize big data: volume, variety, and velocity, or the three V's. The volume of the data is its size, and how enormous it is. Velocity refers to the rate with which data is changing, or how often it is created. Finally, variety includes the different formats and types of data, as well as the different kinds of uses and ways of analyzing the data.

According to Kubick (2012) the leading edge of big data is streaming data, which is collected in real-time from the websites. Some researchers and organizations have discussed the addition of a fourth V, or veracity. Veracity focuses on the quality of the data. This characterizes big data quality as good, bad, or undefined due to data inconsistency, incompleteness, ambiguity, latency, deception, and approximations (TechAmerica, 2012).

Social media has recently become important for social networking and content sharing. Yet, the content that is generated from social media websites is enormous and remains largely unexploited. However, social media analytics can be used to analyze such data and extract useful information and predictions (Asur and Huberman, 2010). Social media analytics is based on developing and evaluating informatics frameworks and tools in order to collect, monitor, summarize, analyze, as well as visualize social media data. Furthermore, social media analytics facilitates understanding the reactions and conversations between people in online communities, as well as extracting useful patterns and intelligence from their interactions, in addition to what they share on social media websites (Zeng, 2010).

Considering that the utilization of data as an advantage by showcase players may interfere with fair competition, it is presented that the Competition Commission of India and Africa has a specific level of duty to advance the use of the right to data protection as well when acting in its ability as a competition authority. The present paper endeavours to go into the essence of the matter and touch base at a conclusion.

Research Methodology

This Research paper receives secondary sources of data through the doctrinal strategy for exploration. Doctrinal Methodology incorporates different sorts of sites, blogs, research papers, newspaper articles and books for reference purpose.

Research Problem

The issue is whether the implications of collection and storage of big data by corporations under competition law adversely affects the privacy of the users. The Competition Act, 2002 has been enacted to prevent activities that have an adverse effect on competition in the Indian Market. The Preamble of the Act unambiguously enunciates the role of 'economic efficiency' in competition law. The goal of competition law is to build a competitive market and thus foster economic growth of the nation.

On the other hand In Africa ,The Competition Commission (Commission) is one of three independent statutory bodies established in terms of the Competition Act, No. 89 of 1998 (the Act) to regulate competition between firms in the market. The other bodies are the Competition Tribunal (Tribunal) and the

Competition Appeal Court (CAC). The Commission is the investigating and prosecuting agency in the competition regime while the Tribunal is the court. The CAC hears appeals against decisions of the Tribunal. Although each of the bodies functions independently of each other and of the State, the Commission and Tribunal are administratively accountable to the Economic Development Department (EDD), while the CAC is part of the judiciary.However, with emergence of the digital economy, the issues relating to 'big data', 'big analytics' & and their implications on competition policy have been raised in the business literature.

Perceiving Data Protection under the Umbrella of Competition Law

The last few years have seen many of the world's leading technology companies come under increasing scrutiny of competition regulators across the globe, with historic fines levied on them for a variety of business practices and other transgressions. The core concerns pertain to accumulation of large data sets by companies and their ability to process it through computer algorithms and artificial intelligence in a manner that may negatively impact competition, as well as the end consumer. Control over this large pool of data is increasingly becoming synonymous with 'market power', even as an increasing number of industries – ranging from agriculture to airlines – become reliant on 'big data'.

Recently, a Committee of Experts (Srikrishna Committee) set up in India to draft a law for data protection in the country after enunciation of the right to privacy by the Indian Supreme Court, released the "Personal Data Protection Bill, 2018". The bill comes against the backdrop of a flagship programme of the government, the Aadhaar Project the biggest ID database of citizen data in the world. Over 79% (87 crore of 109.9 crore accounts) of all bank accounts in the country have been linked to the Aadhaar as of March, 2018 and insurance policies, credit cards, mutual funds, pension plans and social welfare benefits will have to be seeded to the Aadhaar as well. As we enter the age of datafication that entails "*taking all aspects of life and turning them into data*", our ever-increasing financial transactions give away not only our credit history and financial records but also the derivative sensitive information like personality traits, data pertaining to health, product preferences, political, religious and sexual orientation.

The Protection of Personal Information Act (POPIA)2013- Applies to Everyone

The Act applies to any person or organisation who keeps any type of records relating to the personal information of anyone, unless those records are subject to other legislation which protects such information more stringently.It therefore sets the minimum standards for the protection of personal information. It regulates the "processing" of personal information. "Processing" includes collecting, receiving, recording, organizing, retrieving, or using such information; or disseminating, distributing or making such personal information available. The Act will also relate to records which are already in the possession of the entity or person doing the processing. This article must be read in conjunction with the POPI Act No. 4: Protection of Personal Information Act, 2013.

The emergence of big data as an asset for market players does not only raise data protection issues but also leads to competition considerations. The rapid growth of data application in this digitized economy unveils the scope of data protection in the realm of competition law. Data protection and competition law both influence the exercise of economic activity and seek to enhance the interests of individuals. They do this, however, at different ends of the same spectrum: data protection law protects the integrity of individual decision-making regarding personal data processing (for instance, by granting when consent is used as a legal basis for data processing) while competition law safeguards consumers against unlawful exercises of market power.

Competition law in India is enforced primarily by the Competition Commission of India ("CCI"), established under the Competition Act, 2002 ("Act"). The CCI has

the responsibility to "prevent practices having an adverse effect on competition and sustain competition in the market" and has been quite actively enforcing the Act since its inception in 2009. Under the Act, the CCI can look into three aspects: Anti-competitive agreements, including collusive agreements between competitors under Section 3 of the Act Abuse of dominant position by an enterprise under Section 4 of the Act and Regulation of mergers and acquisitions under Section 5 and 6 of the Act. While there has been limited scrutiny by the CCI on issues relating to data, it has, in 2017-2018, passed three orders dealing with the impact and significance of data in the competition landscape which included complaints filed against WhatsApp and Google and approving the merger of Bayer and Monsanto. It is noteworthy – and perhaps an indicator of the things to come – that in 2018, while approving the merger between Bayer and Monsanto, the CCI directed the merged entity to provide agricultural information/data on fair, reasonable and non-discriminatory terms.

The new South African competition law forms an important part of reforms designed to both address the historical economic structure and encourage broad-based economic growth. The government has recently developed the 'Microeconomic Reform Strategy' in which the role of competition policy is identified as central to the efficient outcomesof markets. Competition policy is seen as important in increasing competitive market pressures, leading to firms becoming more efficient and internationally competitive. Itis also viewed as important for the improved participation of black-owned companies in the economy. There is little doubt that corporate ownership and control in the South African economy is highly concentrated. In the latest available manufacturing census (StatsSA, 1996), for46 per cent of the 57 main product groupings the largest four firms account for more than half the output, while in a further 35 per cent of groupings the four firms' concentration ratio is between 0,25 and 0,50.

CCI has the power to impose significant penalties, up to 10% of the average of the turnover for the last three years or in case of a cartel, 3 times of the profit for each year in continuation of a cartel. In case of an abuse of dominant position, the CCI can also direct division of an enterprise. Similarly, while assessing a merger, CCI can direct divestment of certain assets or pass detailed guidelines on carrying of certain business activities, where the merger is found to have or is likely to have adverse effect on competition in India which is Very similar to Africa.

The Act of Africa deals with two main areas: prohibited practices (covered in Chapter 2 of the Act) and mergers (Chapter 3). The prohibited practices are further separated into restrictive practices – either horizontal or vertical – and abuse of a dominant position. The objectives of the Act are broad and take into account a range of concerns that will not necessarily be consistent with each other in the actual evaluation of cases. They are stated in section 2 of the Act as follows:

The purpose of this Act is to promote and maintain competition in the Republic in order:

(a) To promote the efficiency, adaptability and development of the economy;

(b) To provide consumers with competitive prices and product choices;

(c) To promote employment and advance the social and economic welfare of South Africans;

(d) To expand opportunities for South African participation in world markets and to recognise the role of foreign competition in the Republic;

(e) To ensure that small and medium-sized enterprises have an equitable opportunity to participate in the economy; and

(f) To promote a greater spread of ownership, in particular to increase the ownership stakes of historically disadvantaged people.

However, these two fields of law intersect when undertakings compete on the basis of data protection, that is to say, when consumers are influenced by the personal data protection conditions governing the processing of their personal data. Their shared

objectives then pave the way for data protection law to influence substantive competition law assessments. The interaction between data protection and competition law began to gain attention from policy makers and academia after the announcement of Google's proposed acquisition of Double Click in 2007. Concerns were raised mainly owing to the information which would have been in the hands of Google after the completion of acquisition. Most notably, Peter Swire argued in his testimony on behavioural advertising that a "combination of 'deep' information from Google on search behaviour of Individuals with 'broad' information from DoubleClick on web-browsing behaviour of individuals could significantly reduce the quality of Google's search engine for consumers with high preferences." However, despite calls to oppose the acquisition on the grounds of privacy considerations, the Federal Trade Commission (FTC) of the United States stated that it lacks the legal jurisdiction to tether conditions that do not associate with anti trust. In its view, the sole purpose of merger review is to identify and remedy transactions that harm competition. It was contended that FTC could have depended on a different hypothesis to combine privacy issues in competition analysis of the transaction by the then-commissioner Paula Jones Harbour.

The discourse got revitalized when Facebook announced its acquisition of WhatsApp in 2014 which was approved by both the US FTC and the European Commission (EU). The EU reiterated that any privacy related concern as a result of the transaction does not fall within the scope of EU competition law but within the ambit of EU data protection laws. In spite of oppositions to both the Google/DoubleClick and the Facebook/WhatsApp transactions, the US FTC as well as the EU decline to include privacy-related concerns into competition law and state that privacy-related concerns should rather be resolved under data protection laws.

Data has been recognised as a non-price parameter in competition assessment in the Microsoft/LinkedIn merger, if it is a significant factor in the quality of services rendered. In the digital era, big data helps enterprises in improving the services rendered by them and providing more customized options based on the individual preferences. However, at the same time, it raises privacy-related concerns which should not be ignored.

Eu Data Protection Framework

EU data protection law is comprised of a mixture of primary and secondary law. Article 16 TFEU provides an explicit legal basis for EU data protection legislation while Article 8 of the EU Charter sets out a right to data protection. At present, the 1995 Data Protection Directive regulates personal data processing; however a General Data Protection Regulation (the GDPR)[1] will replace this Directive in May 2018. The GDPR seeks to clarify existing rights and obligations while introducing changes to improve compliance and enforcement. This secondary law must be interpreted in light of the EU Charter rights to privacy and data protection.

The EU data protection framework has a broad scope of application, as it applies to personal data processing conducted by natural and legal persons and public and private bodies, with limited exceptions.[2] Personal data is defined as any information relating to an 'identified or identifiable individual and processing as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means.[3] Personal data processing is permissible provided it has a legal basis and also complies with certain safeguards. The most well-known legal basis for processing is the consent of the individual 'data subject, however there is no hierarchy amongst the six legal bases listed. Processing is therefore equally legitimate if, for instance, it is necessary for compliance with a legal obligation or for the performance of a contract. Of the safeguards, the so-called 'purpose limitation' principle should be highlighted. According to the principle, personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. The framework also provides individual data subjects with rights over their personal data, for instance, the right to information regarding the processing of their

personal data[4], the right to delete personal data in certain circumstances and the right to access personal data.[5] Through this framework, data protection determines the boundary between permissible and impermissible personal data processing and, in so doing, reconciles individual rights with other societal interests.

Technology companies in India and Africa: Understanding the ramifications under India's competition Legal framework

Personal data has become the object of trade in the digital economy, and companies compete to acquire and process this data. This rivalry is subject to the application of competition law. However, personal data also has a dignitary dimension which is protected through data protection law and the EU Charter rights to data protection and privacy. Data, which has not been ascertained as a competitive concern, is a major source of power today. The regulators in the EU are keeping a close eye on how Big Data companies are making use of such data. It will therefore not be surprising to see new rules modifying the turnover thresholds in the merger regulation or additional guidelines on article 102 TFEU specifically in relation to data holding companies. The EU competition commission's indication to adapt new rules signals a significant policy change in its approach to handle Big Data.[6]If such indications materialize, the EU Commission will have empowered itself enough to deal with Big Data entities like Facebook and Google which have traditionally been dealt with in the sphere of data protection alone.

Broadly speaking, the primary concerns that arise due to the interplay of data collection, processing and transfer, and competition law in the Indian context are identified here:

1. Collusive Behaviour: Any technological platform enabling 'real-time' access to price and quantity data is viewed with suspicion by competition regulators Possibility of collusion between competitors using a 3rd party developed algorithm or AI, which relies on data sets or 'real-time data'. This poses new & legal compliance challenges for the enterprises, diminishing the lines between permitted and prohibited conduct.
2. Possibility of Abuse: Any abuse of market power arising out of control over data may raise concerns such as: Access to data can be used to implement entry barriers against other participants in the market Discriminatory access to such data may also raise potential red flags Concerns may also arise from exclusive agreements if they prevent other entities from accessing data or foreclosing rivals' opportunities to procure similar data, by making it harder for consumers to adopt rival technologies or platforms.
3. Big data in mergers: Any abuse of market power arising out of control over data may raise concerns such as: Access to data can be used to implement entry barriers against other participants in the market Discriminatory access to such data may also raise potential red flags Concerns may also arise from exclusive agreements if they prevent other entities from accessing data or foreclosing rivals' opportunities to procure similar data, by making it harder for consumers to adopt rival technologies or platforms.

Data Protection Interests in Merger Review

Mergers are regulated by sections 5 and 6 of the Indian Competition Act. Section 6 prohibits any combination which causes or is likely to cause an appreciable adverse effect on competition within the relevant market in India. Data-related competition issues cannot always be identified using the current distinction made between horizontal, vertical and conglomerate mergers. Even if a merger does not lead to a horizontal or vertical overlap and does not give rise to conglomerate effects in terms of the products and services that are offered by the merging parties, a combination of datasets may still have a competitive impact. The obtained datasets provide an opportunity to an enterprise to improve existing products and to develop new products, i.e. entering into another relevant market. Since no real market for supply and

demand of data exists, it becomes quite difficult for competition authorities to tackle such issues. However, by defining a potential market for data as an asset, authorities would be able to tackle competition concerns relating to datasets or data concentration in merger cases. This might be considered as a big step in merger review as the datasets act as a super asset in the combination cases in the online market. In a March 2016 speech, EU Competition Commissioner stated: "Sometimes, what matters are its assets. That could be a customer base or even a set of data".

Section 16 of the Africa's Competition Act sets out the statutory standard for merger evaluation. This includes assessing competition in the identified market, taking into account the actual and potential level of import competition, ease of entry, countervailing power, as well as the removal of an effective competitor. Technological and efficiency gains that could offset any potentially anticompetitive effects resulting from the merger are also considered. Public interest issues that may be taken into account include employment; the ability of small businesses, or firms controlled or owned by historically disadvantaged persons, to become competitive; and the ability of national industries to compete in international markets. These are, however, secondary concerns that may be set against competition implications if they are deemed to be very significant. Several mergers that have increased concentration have been approved with conditions. The power of the Tribunal has been exercised in these cases by its analysis of factors determining economic efficiency over time. International competitiveness and economies of scale were taken into account in allowing the mergers of Trident Steel and Baldwins Steel, and Iscor and Saldanha. The need for consolidation in the face of increased international competition and/or a failing firm underpinned qualified approval in many other cases.

The need for a potentially relevant market for data can be illustrated by reference to the Google acquisition of Nest in 2014. Nest, a producer of smart home devices and Google, a search engine, were not competing in any relevant market. Nevertheless, this acquisition benefited Google as it acquired the access to data on the behaviour of consumers, which in turn must have benefited Google in developing the services rendered by it or in developing a new product. The US FTC, which cleared the deal, would have been able to assess such concerns in greater detail had it defined the potential market for data. In a data-driven economy, such merger has the potential of restricting the concentration of relevant data and create entry barriers for new companies as they do not have access to such amount of relevant data leading to obstructing their expansion and in turn to eliminating competition. Merger in the data-related economy can also lead to vertical or conglomerate effects if a large enterprise has obtained the ability to restrict upstream or downstream competitors' access to data. More generally, vertical integration can entail discriminatory access to strategic information with the effect of distorting competition.

Fundamental right to data protection in antitrust investigations

Most competition authorities can raid businesses and private premises in order to obtain documents that evidence presumed infringements of competition law. They have the power to conduct "all necessary inspections", meaning that the investigation decision must be based on reasonable grounds and aimed at verifying the existence and scope of a presumed infringement based on already available information. Fishing expeditions are not allowed[7]

"E-discovery" in the course of dawn raids and related problems regarding seized private data. The right to privacy, which comprises the right to data protection, is especially at risk when competition authorities examine virtually the entire IT environment of an undertaking. When sifting through hard copy documents, a quick look at the document often allows the investigator to identify whether it is exempted from review. This does not hold true for masses of digital information seized and later examined by the authority, leading to a critical tension between "e-discovery" measures and the right to data protection.

Constitutional privacy protections: Section 14 of the Constitution of the Republic of South Africa protects the right to privacy. Data protection laws: The Protection of Personal Information, Act 4 of 2013 (POPI) is the primary instrument regulating data protection in South Africa. Data protection agency: Section 39 of POPI establishes the Information Regulator, a body composed of several members. Among the Information Regulator's duties are monitoring and enforcing compliance and handling complaints related to the enforcement of privacy laws.

The Volker and Markus Schecke GbR /Land Hessen case would suggest that the right to data protection only applies in a very restricted way to legal persons. However, the right to data protection of natural persons also can be affected, especially the "blind" confiscation of whole mailboxes, which can include private correspondence. While it has been confirmed that an e-discovery as such does not violate the right to privacy, such measures have to be proportionate. Confiscation of masses of electronic data which include private data is thus only admissible if:

(i) the confiscation itself is related to the alleged infringement and not arbitrary (e.g. restricted to the employees working in the field of the activity concerned);

(ii) the investigated undertaking is provided with a copy as well as a report of the seized data; and

(iii) the authority was not able to filter the seized data more stringently. The technological possibilities of further selection will therefore be decisive for the legality of e-discovery measures. Widespread and indiscriminate confiscation of IT data is prohibited. The undertaking must also have the possibility to object to the confiscation.

Besides data protection being a fundamental right that every competition authority needs to respect, stricter data protection rules are believed to facilitate customer choice and ultimately benefit consumer welfare, which is at the heart of competition policy. Proponents of giving more weight to privacy considerations in antitrust assessments claim that privacy rules are a significant aspect of the quality of (often free) services offered by the digital industry, valued highly by consumers, but treated sluggishly by the dominant players owing to the power imbalance between the former and the latter. The more powerful the company in the digital industry, the more the level of data protection is believed to be at risk, with authorities being ill-equipped to assess these issues with their current economic toolset. Antitrust policy should actively encourage privacy competition, because high entry barriers due to several data-driven network effects and the incumbent's behaviour prevent the emergence of competing service providers that offer better privacy policies.

Data Protection Interests and Abuse of Dominance

Data may play a significant role in establishing dominance. It is argued that "a serial disregard for the privacy interest of consumers forms an indication that an undertaking has the power to behave independently in the market and thus possesses a dominant position". However, it is not necessary that existence of data is always detrimental to consumer welfare if privacy forms only one aspect of quality and works as a currency for more relevant end-products and services. Nevertheless, a dominant position can be established if data protection is the only aspect of quality and does not interrelate with other product dimensions.

In Africa the abuse of a dominant position by a firm may include excessive pricing of goods or services, denying competitors access to an essential facility, price discrimination (unjustifiably charging customers different prices for the same goods or services) and other exclusionary acts (such as refusal to supply scarce goods to a competitor, inducing suppliers or customers not to deal with a competitor, charging prices that are below cost so as to exclude rivals, bundling goods or services and buying up a scarce input required by a competitor).The Act prohibits the abuse of a dominant position by firms in a market, but does not prohibit firms from holding a dominant position. The hurdle for proving abuse of dominance cases are significant, they require extensive legal and

economic analysis. This is evident in the small number of cases where abuse of dominance has been found and the extensive evidence that has been required for these findings. Firstly, proving allegations of an abuse of a dominant position require proof that the respondent is dominant. The Act uses both market share and market power to define dominance. Market power is the ability of a firm to behave in a manner that does not take into account the reactions of its competitors, customers or suppliers, or to control prices. Secondly, there must be evidence that the respondent is abusing its dominance.

From a competition perspective, the question which arises is: what amount of data is to be considered as excessive to establish dominance? An approach that can be followed involves the use of a data protection benchmark against which the existence of abusive behaviour can be tested. By using this principle, data protection can be integrated in competition law for assessing abuse of dominance [such approach was used by Bundeskartellant (German competition authority) when they announced the commencement of proceedings against Facebook]. Data can also facilitate price discrimination as a large amount of data helps in analysing the preferences and reservations of the consumers which helps the companies in adapting the prices to individual customer groups.

Conclusion, Suggestions and Recommendation

Although, 'big data' has been the centre of attention from competition regulators globally, the authorities are still in the process of gaining a better understanding of inherent issues and ascertaining the manner in which the traditional tools can be applied to a technology driven landscape. The vulnerability to competition law scrutiny as a result of data accumulation and processing, extends across sectors ranging from the obviously vulnerable businesses (such as, aggregators, social networks, search companies) to businesses in traditional sectors (hospitality, insurance, life sciences, etc.). It would be prudent for companies to follow basic hygiene measures, including a regular review of existing policies, practices and agreements pertaining to data collection /processing/access in order to identify possible competition compliance gaps and risks involved; seeking specialist advice on issues pertaining to M&A activity; ongoing negotiations with parties in relation to data collection; streamlining policies, practices and contracts with applicable legal requirements; etc. Even though limited information and jurisprudence is available in India, given the nascent nature of competition laws framework in the country, it is quite possible to assess potential competition issues that can arise for technology and data intensive companies in India, and recommend suitable measures to limit such potential regulatory risks. Pre-emptive risk assessment and proactive mitigation steps are indeed the need of the hour.

On African point of view, High levels of concentration mean that there are great analytical demands on competition institutions in relatively small developing countries such as Africa, even though their capabilities in terms of information gathering and analysis are weaker than those of their industrialised counterparts.

Even though competition authorities are currently reluctant to integrate data protection into competition, it is submitted that greater consideration should be given to data protection. The competition authorities need to go beyond the school of thought of justification of competition, i.e. the concept of 'economic efficiency' while assessing the merger and abuse of dominance cases which involve data on a large scale. Competition authorities need a balanced approach between 'economic efficiency' and 'data protection'. However, at the same time, it should be noted that competition and data protection law are two different legal regimes having different causes of concern. This implies that pure data protection issues should be considered by data protection authorities. Considering that the utilization of data as an advantage by showcase players may interfere with fair competition, it is presented that the Competition Commission of India has a specific level of duty to advance the use of the right to data protection as well when acting in its ability as a competition authority.

Africa in conclusion has to focus on improving economic evaluation of firm behaviour by the competition authorities, as well as on the different measures that could be employed to impact on the nature of interfirm rivalry and behaviour, suggests the need to develop links between the competition authorities and other public institutions that have strong information-gathering and analytical capabilities. There may have been an overemphasis on the separation of the competition institutions for fear of their independence being compromised. However, without improved abilities to collect and interpret information, and develop applicable remedies, they will remain relatively ineffective in addressing the effects of existing concentrations.

While Indian law does not allow the convergence of competition and privacy concerns, the European Commission rightly accords centrality to consumer welfare in accounting for privacy concerns in its evaluation of mergers. Anti-competitive effects of data aggregation affecting the quality of services or goods offered as well as privacy protection by the concerned companies will be part of a deal's competition assessment by EU regulators.

Even the regulation averse U.S. FTC directed the divestiture of a significant database prior to allowing Dun & Bradstreet to acquire Quality Education Data in 2010. A joint study by the French Autorité de la concurrence and the German Bundeskartellamt on big data and competition law concerns discusses the nexus between privacy concerns and increased market power due to big data.

This research paper for this international conference gives a way to understand the challenges and barriers faced by business establishments in respect to its competition. A sufficient light is thrown on consumer welfare and efficiency that indirectly regulates the working of business economy. As big data and its analytics are as such resulting to social and economic evils.

The recommendations to place proper stiffer and gatekeeper to supervise and administer all business activities. Thus, competition proceedings should ideally overlap with and cover data protection laws, more so in the merger control of companies which collect and processes large swathes of data through mergers have been expressly exempted from users' consent requirement. Similarly, the implications of collection and storage of big data by corporations upon degradation in privacy protection, product quality and competition by creating new gatekeepers and stiffer barriers also merit antitrust regulation in India's data rich landscape.

References

- Asur, S., and B.A. Huberman (2010). Predicting the Future with social media. In: ACM International Conference on Web Intelligence and Intelligent Agent Technology, vol. 1, pp. 492–499.
- TechAmerica (2012). Demystifying Big Data: A Practical Guide to Transforming the Business of Government. In: TechAmerica Reports, pp. 1–40.
- EMC: Data Science and Big Data Analytics. In: EMC Education Services, pp. 1–508 (2012)
- Russom, P. (2011). Big Data Analytics. In: TDWI Best Practices Report, pp. 1–40.
- Kubick, W.R.(2012). Big Data, Information and Meaning. In: Clinical Trial Insights, pp. 26–28.
- Zeng, D., Hsinchun, C., Lusch, R., Li, S.H.(2010). Social Media Analytics and Intelligence. IEEE Intelligent Systems, 25(6), 13–16.
- The Constitutional law of India- J.N. Pandey, 50thEdition.
- The Constitutional Law of India- M.P.Jain, Levixnexis, 25th Edition.
- Information and Technology – Vakul Sharma, 4thEdition.
- Guide to Competition Law- S.M. Dugar, Volume 1 &2.
- https://www.compcom.co.za/abuse-of-dominance/