COMPETITION LAW IN THE DIGITAL SECTOR: A STUDY OF DIGITAL PERSONAL DATA PROTECTION BILL, 2022

- VINITA SINGH, VINAYAK SANJAY BUCKSHEE[*]

ABSTRACT

In terms of data regulation, competition agencies play a significant role. Digital business giants gather huge amounts of data related to their customers. These enterprises can engage in data-driven innovations because of access to data. This in turn enables them to make more accurate assessments of consumer needs, demands, and preferences. As a result, having access to data can provide a competitive edge. A data-rich competitor can improve its service and make it more user-targeted in order to strengthen its market dominance. A business that has a huge user base can gather more data to enhance the value of its service and draw in new customers. Additionally, businesses can use user data to enhance targeted advertising and monetize their services, gaining extra money to improve the service's quality and luring back more customers - a process known as the 'monetisation feedback loop.' This loop can make data access act as a barrier to digital market entry. Therefore, the anti-trust legal framework is a crucial regulatory tool to combat the exploitative and restrictive behaviour caused by the gathering of data by companies with market dominance. This paper keeping the Market Study Report on the Telecom Sector in India released by the CCI in January, 2021 in consideration, is aiming to study the interplay between data privacy and competition regulation vis-a-vis the Draft Digital Personal Data Protection Bill, 2022.

[*] Ms. Vinita Singh and Mr. Vinayak Sanjay Buckshee are students at Damodaram Sanjivayya National Law University, Visakhapatnam.

I. INTRODUCTION

Unlike the separatist view which considers competition law and data protection law separate and independent, the integrationist theory suggests that privacy and competition law are complementary and can be integrated together.[1] When evaluating a corporation's operations and their influence on market competition, market efficiency and consumer welfare, privacy and the protection of personal data are not to be considered as secondary issues. Instead, they are primary considerations.[2] Consumers are data subjects, and their welfare may be in danger if dominant enterprises restrict their ability to choose and exercise control over how their personal information is used. The goal of data protection is to preserve people's fundamental freedoms and rights without limiting the free flow of private data. Market value and competitive advantage are conferred by data. As a result, there will undoubtedly be more data collected and processed as a result of the rising thirst for data. Consequently, there would be less online privacy and increased profiling and insight into customer preferences.

Most of the digital markets show very strong economies of scale.[3] The marginal costs of copying and online distribution are low to non-existent for software and digital material contrary to their fixed development expenses. Hence, unit costs are usually inversely proportional to sales volume, affording the dominant market firm a significant competitive advantage. Several digital services perform communication or linking tasks, resulting in network effects that are both direct (within-market) and indirect (cross-market).[4] Although they exist in other sectors as well, digital markets are where they are most common and significant.

[1] Arletta Górecka, 'Competition Law and Privacy: An Opinion on The Future of a Complicated Relationship' (Kluwer Competition Law Blog, 3 April 2023) <https://competitionlawblog.kluwercompetitionlaw.com/2022/06/08/competition-law-and-privacy-an-opinion-on-the-future-of-a-complicated-relationship/>accessed 3 April 2023.

[2] European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) < https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 3 April 2023.

[3] Antonio Capobianco, 'The Evolving Concept of Market Power in the Digital Economy – Note by Brazil' (2022) Organisation for Economic Co-operation and Development. <https://one.oecd.org/document/DAF/COMP/WD(2022)31/en/pdf> accessed 3 April 2023.

[4] T P Barwise and L Watkins, *The evolution of digital dominance: how and why we got to GAFA. In: Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (OUP 2018).

Digital technology makes it possible to collect and automatically analyse usage data on a massive scale in real time. This data may be used tactically and strategically, particularly through continued personalization and quality management.[5]

The Ministry of Electronics and Information Technology presented the Digital Personal Data Protection Bill (***hereafter, 'Bill'***) on November 18, 2022. With the idea of coming up with a comprehensive data protection law, India has proposed a privacy law four times since 2018.[6] The proposed Bill's objectives include ensuring that digital personal data is processed in a way that respects both individuals' right to privacy protection and the necessity of processing personal data for legitimate purposes.[7]

II. DIGITAL PERSONAL DATA AND COMPETITION LAW

A. Data and Market Dominance

Customer data is always valuable for a business but it is especially more important for digital platforms. This is because digital platforms are far more accessible compared to traditional businesses and digital businesses are better equipped to process and utilise that data for several uses. Learning about the tastes and preferences of consumers helps to match supply and demand while cutting down on waste and transaction expenses.[8]

Digital platforms make it easier for companies to find customers, monetize underutilized assets, and reduce transaction costs.[9] Instead of following consumers around to observe their buying activity, an online website can more easily monitor which products consumers have clicked on.

---

[5] Ibid.

[6] Trishee Goyal, 'A First Look At The New Data Protection Bill' (*The Hindu*, 20 November 2022) <https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece> accessed 3 April 2023.

[7] Ibid.

[8] Yogesh K Dwivedi, 'Setting The Future of Digital and Social Media Marketing Research: Perspectives and Research Propositions' (2021) vol 59 < https://www.sciencedirect.com/science/article/pii/S0268401220308082 > accessed 4 June 2023.

[9] ITIF 'ITIF Technology Explainer: What Are Digital Platforms?' (ITIF, 12 October 2018), <https://itif.org/publications/2018/10/12/itif-technology-explainer-what-are-digital-platforms/> accessed 3 April 2023.

If a platform dominates the market, it will have more users than its competitors and, as a result, more extensive consumer data. The dominant company may be able to make information-dependent product enhancements because of the larger data set, which smaller competitors will not be able to match.

It is the utilisation of data gathered that determines commercial success of a corporation to a great extent. Suppliers are urged to keep a record of everything in order to assist with various possible applications of artificial intelligence like target marketing customization, price discrimination, and risk analysis. On one level, more data is beneficial for these uses. Machine learning algorithms need a lot of data input. It is using millions of data input on market users and opportunities for market expansion.[10] Major leading companies use the mechanism of surveillance capitalism which gathers private data of their customers and use it to generate profit by improving its service accordingly.[11] Large amounts of personal data can give a dominant company a competitive edge, depending on when returns on extra consumer information start to decline. Access to the largest proportion of customer data could help a company gain market dominance if the advantages of more information only start to diminish at very high data numbers and if relative disparities in access to customer data are by a significant margin. Customers may stay with the leading digital site due to network effects, switching costs, or general preferences in which case the site's exclusive access to a sizable portion of consumer data may help it preserve its dominant market position.[12]

B. Concealed Data

[10] Wolfie Christl, 'Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions' (2017) Cracked Labs. <https://crackedlabs.org/en/corporate-surveillance> accessed 3 April 2023.

[11] Donell Holloway, 'Explainer: What Is Surveillance Capitalism And How Does It Shape Our Economy?' (The Conversation, 24 June 2019), <https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158> accessed 3 April 2023.

[12] 'The Evolving Concept of Market Power in Digital Economy' (2022) OECD Competition Policy Roundtable Background Note < https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf> accessed 3 April 2023.

Data collection is utilised to improve business efficiency and product quality that has benefited people in numerous ways. However, more often than not, the people whose private data is being gathered are unaware of nature, the very value of data being appropriated.[13]
Consumers today deal with the widespread and concealed gathering of their personal information by companies along with the growing number of plans to expand data disclosure and tracking. There is a constant monitoring done of users, either through the credit cards they use or websites they visit on their mobile phones.[14] Even things as basic as home appliances if connected with internet, are subject to tracking.

In this situation, suppliers tend to obtain consent to the collection of a broad range of specific private data about many consumers.[15] In order to avoid consumers being concerned about these activities and disapproving it, companies frequently employ covert technologies to track, and conceal their data techniques from the customers who are being monitored.[16]

"Concealed data practices" occur when suppliers' terms provide weak privacy protections for consumers while the extent of those terms, the resultant data practices and the consequences of these data practices are concealed from consumers.[17] These vague terms often lead to the collection and use of personal data above and beyond what is required for the delivery of the relevant service and what the customer may reasonably expect. Numerous privacy regulators and competition regulators globally looking into the type of competition in digital economy, have raised concerns about practices of this kind in the market.[18] Owing to the absence of power to negotiate and sufficient know-how of the data model being used, consumers initially

[13] Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34(2) Computer Law & Security Review 289.
[14] David Murakami Wood and Kirstie Ball, 'Part A: Introducing the Surveillance Society' (2006) A Report on the Surveillance Society < https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf> accessed 4 June 2023
[15] Alessandro Acquisti, 'The Economics of Personal Data and Privacy' (2010) OECD Joint WPISP-WPIE Roundtable Note < https://www.oecd.org/sti/ieconomy/46968784.pdf> accessed 3 April 2023.
[16] Jan Whittington and Chris Jay Hoofnagle, 'Unpacking Privacy's Price' (2012) 90 North Carolina Law Review 1327.
[17] Katharine Kemp, "Concealed Data Practices and Competition Law: Why Privacy Matters" (2020) 16 European Competition Journal 628.
[18] 'The Right to Privacy in the Digital Age Report' (2014) United Nations High Commissioner for Human Rights < https://unece.org/sites/default/files/2021-09/A_HRC_48_31_AdvanceEditedVersion.pdf> accessed 3 April 2023.

encounter difficulties in understanding the terms of privacy policy and subsequently regulating their privacy.[19]

C. Data Portability

The use of algorithms and the efficient operation of machine learning are made possible by access to suitable datasets for commercial organisations. Businesses can continuously innovate, advance their R&D, and develop distinctive prospects for monetisation by strategizing use-cases using data processing and the inferences obtained from previous user interactions.

While the data accumulated over time boosts the companies' position in the market, the non-availability to pertinent consumer databases can affect budding and emerging rivals. This may serve as a barrier to entry that is amplified by the presence of powerful network effects.[20] Additionally, businesses exploit the data they collect and process to over-personalize their user interfaces, which increases the switching costs. Given the difficulties in duplicating the data and its worth to a different service provider, these expenses are related to consumers encountering resistance when attempting to cut ties with their present service providers.

By enabling customers to manage their data and move it to different service providers, data portability is considered to lower these switching costs. By providing competition and improved technology to the markets, their incorporation in the law can contribute to greater competitiveness, product improvement, and overall growth.

III. CCI TELECOM REPORT

The Competition Commission of India (CCI) in tandem with the Indian Council for Research on International Economic Relations in January 2021 released its report on market study of the Telecom Sector in India.[21] It analyses recent developments, threats, and challenges to competition in India in the digital field.

---

[19] Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA Law Review 606.

[20] Shubhangi Heda, 'Contours of Competition Policy in the Digital Economy' (2021) vol 8, Indian Competition and Regulation Report < https://cuts-ccier.org/pdf/Report-ICRR2021.pdf > accessed 4 June 2023.

[21] CCI, 'Market Study on the Telecom sector in India' (22 January 2021) <https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf> accessed 3 April 2023.

The CCI analysed the relationship between data privacy and market competition. The report discusses the possibility of market abuse that can arise from the weak data privacy provided by dominant business in market. Integrating the data accumulated with other digital products strengthens the already resting competitive edge with the leading enterprises. It stated that a high combined data share can lead to market power, subsequently resulting in entry barriers leading to rise in switching cost and that adversely impact other market players.[22] It found a case-by-case analysis well suited for deciding whether the collection of "excessive amounts" of data can be anti-competitive. The friction between giving access and safeguarding consumer privacy is another dimension of data with regards to market competition in the digital communications sector. Privacy can play a significant role in non-price competition.

It suggested establishing line of communication between the DoT, the TRAI, the CCI and the envisaged Data Protection Authority to enforce consistent and effective regulatory decisions. It also emphasized on the significance of inter-regulatory consultation mechanism in Sections 21 and 21A of the Competition Act.[23]

IV. DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Laws governing data privacy systematically control how people's data is used. Hence, data privacy legislation deals with one's right to control their personal information.[24] Information privacy is a type of the broader concept of privacy. Privacy can be bodily in nature like bodily autonomy and it can be geographical like territorial privacy. Information privacy, commonly called data privacy, seeks to protect personally identifiable information (PII) stored in a computer system.[25] Data privacy protects data in transit and data at rest without disrupting free flow of information. Regulation in the domain of information privacy is heavily influenced by the ideas of notice and consent.

[22] Ibid.
[23] Ibid.
[24] Katharine Kemp, 'Concealed Data Practices and Competition law: Why Privacy Matters' (2020) 16 European Competition Journal 628.
[25] Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.

Among the key changes proposed as compared to the 2019 and 2021 Data Protection Bills are its applicability, deemed consent, cross border transfers and penalty provisions. Another significant way in which the draft Bill differs from previous ones is the elimination of the category of sensitive personal data. This often comprises financial, genetic, and biometric information, all of which call for higher levels of protection. Yet, it seems that the present proposal offers a lowered protection for personal data by discarding this categorization.

A. Data Portability

The Bill 2022 provides Data Principals with rights of seeking information under broad categories like data summary, information on other data fiduciaries with whom data is being shared etc. However, one of the major shifts from the previous drafts (2018 and 2019)[26] has been the dilution of the right to data portability. Data Principals cannot seek copies of their personal data in portable form that would have potentially allowed them to switch platforms. Additionally, the right to be forgotten has also not been provided as per the Draft Bill. After reviewing the 2019 Bill, the Joint Parliamentary Committee had suggested keeping these rights.[27] These rights are likewise acknowledged by the General Data Protection Regulation (GDPR) of the European Union.[28] The Srikrishna Committee (2018) also considered Data Portability rights a crucial element of a data protection law. To provide people control over their data, these rights are founded on the concepts of autonomy, transparency, and accountability.

The right to data portability entitles data principals to receive and transfer their data in a structured, widely accepted, and machine-readable format from a data fiduciary for their own use.[29] It allows the data principal better control over their data and can enable Data Principals to switch from one data fiduciary to another. Particularly, data portability can practically lower the costs associated with switching suppliers for consumers, as opposed to the case where the users would be required to restructure all of their data and content that has been supplied, into

[26] Clause 26, The Personal Data Protection Bill, 2018; Clause 19, The Personal Data Protection Bill, 2019.
[27] Report of the Joint Committee on The Personal Data Protection Bill, 2019 (December 2021), Para 1.15.13.
[28] General Data Protection Regulation (EU) 2016/679, Article 20.
[29] Alberini and Adrien, 'Data portability and interoperability: an issue that needs to be anticipated in today's IT-driven world' (2017) Expert Focus.

a digital content platform every time they change service providers.[30] Customers may be able to enter new businesses, increasing competition, if they are able to bring their data with them. Comparison services in areas with complex price structures can also be made possible through data portability.

With the Draft Digital Personal Data Protection Bill 2022 removing right to data portability, it may have an adverse impact on the market competition. If a dominant company has private data of its users that are required by other companies to enter the market, then in that case, the refusal to share such data by the dominant company can result in the elimination of all potential market competition. The dilution of the right to portability in the Draft Bill 2022 brings numerous consequences to the market competition like bar to market access, high switching cost and exclusionary abuse of dominant position by certain companies.

B. Consumer Consent

Suppliers often use privacy policies to grant themselves the power to alter privacy conditions without taking consent from the customers[31], and they put a responsibility on customers to check the supplier's website regularly for such changes. It is practically impossible for any consumer to become aware of the new conditions in this way given that multiple suppliers have privacy policies that apply to a single consumer. Lowering privacy protection is one way how abuse of dominance can manifest itself, and as such, falls under the purview of antitrust laws since a lack of consumer welfare is implied by a low privacy standard.[32]

Taking example of other countries, Japan has come up with finalised guidelines as per which, using personal data of users like purchase history and location, without their prior consent can

[30] OECD, 'Data portability, interoperability and competition', (2021) OECD <https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm> last accessed 10 March 2023.

[31] Gianclaudio Malgieri and Bart Custers (n 6).

[32] CCI, 'Market Study on the Telecom sector in India' (22 January 2021) <https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf> accessed 3 April 2023.

result in an "abuse of a superior bargaining position."[33] It is a violation contained under the Japan's Anti-Monopoly Act.

The Draft Digital Personal Data Protection Bill 2022 allows processing of personal data only for a lawful purpose and only after obtaining the consent of the individual.[34] A notice containing details about the personal data to be collected and the purpose of processing has to be given before taking consent of the user. The users have been provided with the right to withdraw consent at any point of time.

The Draft Bill additionally provides for a deemed consent provision wherein consent will be deemed given where processing is necessary for: (i) performance of any function under a law, (ii) provision of service or benefit by the State, (iii) medical emergency, (iv) employment purposes, and (v) specified public interest purposes such as national security, fraud prevention, and information security.[35] The Bill treats private and public companies differently when it comes to consent and storage limitations even when they carry out the same commercial purpose.

These provisions put an obligation on companies to obtain consent from users before processing personal data. It restricts the data advantage any dominant company may enjoy by lowering its privacy protection granted to its users. This way, users will have a say in what all personal data can be used by business for improving their services and resultant competitive edge in the market. However, users do not have any control over matters for which consent will be deemed to have been taken.

V. CONCLUSION

Competition law and data protection play a major role in digital economy system. With consumers' data increasingly becoming relevant in the functioning of digital business, it is

[33] JFTC, Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act on the Transactions between Digital Platformer Operators and Consumers that provide Personal Information, etc. (2019) Japan Fair Trade Commission (JFTC) <https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217_DP.html> last accessed 10 March 2023.

[34] Digital Personal Data Protection Bill 2022, s 5.

[35] Digital Personal Data Protection Bill 2022, s 8.

important to balance data privacy and its related impact on market competition. With the Draft Digital Personal Data Protection Bill 2022 recently released with certain changes compared to its earlier versions, it is important to analyse the governance of private data in hands of digital enterprises. The different proposals as contained in the Bill can have varied implications on market competition. It is important to consider the interplay between data privacy regulations and its immediate effect on competition in the digital sector. Policies need to be framed after consultation with sectoral regulators for a fair competition and customer welfare. It is important that significant changes that are required be made in the Bill that will not only protect people's private data but also ensure that the resultant effect on competition in the economy is well balanced.