DATA PRIVACY AND COMPETITION LAW IN INDIA

Kapil Mudgil, Ex. Research Associate, Competition Commission of India

ABSTRACT

In the present digital era, the protection of personal data and the promotion of fair competition are two crucial objectives. In India, these goals are pursued through the Digital Personal Data Protection Act, 2023 ('DPDP Act') and the Competition Act, 2002 ('Competition Act'). While these legal frameworks serve different purposes, they intersect in their approach to data collection, processing, and user consent. Data privacy legislation *i.e.* DPDP Act is intended to protect individuals' personal data, whereas the Competition Act is envisioned to encourage fair and open competition in the marketplace. The harmonious convergence of the DPDP Act and the Competition Act is crucial for striking a balance between data protection and market competitiveness. By fostering collaboration, addressing legal complexities, and embracing the digital era, India can achieve a dynamic legal landscape that propels both creativity and fair play. This article will ponder upon the relationship between data privacy and competition law, as well as the ramifications for firms and consumers.

Data Privacy and Competition Law in India

What is data, exactly? Why there is a hue and cry about big data? Data, by definition, is a collection of qualitative and quantitative variables. We have all heard of government, research, or survey organizations gathering and processing data for various research, policy, and business purposes. In the digital age, however, the notion of 'data' has taken on additional dimensions. In the online world, every click, comment, text, tweet of ours is generating personal data on our preferences, interests, needs and wants. In other words, it is consumer behavior data, which is continuously extracted from online activities of individuals and not a single static data set. Thus, a deluge of data is engulfing the online world. No wonder, why the huge datasets that are generated as a result, are known as Big Data.

Data can also be used to gain market power. A company with a large user base can collect more data to improve the service (for example, by developing better algorithms) and thus attract more customers. Companies, on the other hand, can use user data to improve ad targeting, obtaining additional funds to invest in service quality, and attracting even more users. Big data can provide leaders with additional decision-making resources and insights. Unfortunately, it also poses a challenge to competition law, as companies may use Big Data to gain a competitive advantage. Furthermore, businesses can use Big Data to identify potentially anti-competitive practices such as price fixing or collusion with other businesses to maintain monopolies in specific markets. Knowing more about customers can help businesses, but it can also cause privacy concerns. Businesses can gather enormous amounts of information about their customers, their shopping habits and preferences, and even their biometric data, using everything from rewards programs to apps. This is where the Competition Commission of India ('CCI') comes in. The CCI was established in India under the Competition Act, 2002[1] (the 'Competition Act') to prevent anti-competitive practices, promote and sustain competition in markets, protect consumers' interests, and ensure the freedom of trade practiced by other market participants.

Like in any other sector, market power or dominance *per se* is not an antitrust concern even in data-driven digital markets. It is the practice adopted by dominant digital players that need to be

[1] https://www.cci.gov.in/images/legalframeworkact/en/the-competition-act-20021652103427.pdf

competition compliant. Recently the processing (collection, transfer and holding) of data has been made an element in potential abuse of dominant position cases in several jurisdictions. Processing of data sometimes lead to informational privacy. Privacy is a complex and amorphous concept. It is difficult to demarcate what would amount to loss of privacy as it is often intangible and subjective. In the competition law discourse, it is often said that privacy is a quality factor for online services. The question that is being debated is – could there be an abuse of dominance when excessive data is extracted for reasons other than improving quality or reducing cost? One school of thought is that abuse of dominance can take the form of lowering the privacy protection, privacy issues in the digital markets fall under the purview of competition authorities and competition law is sufficiently wide in scope and armed with tools to deal with these issues in protecting consumer interest. The other school of thought believes that privacy is fundamentally a consumer protection issue. In theory, antitrust can deal with privacy as a non-price factor of competition, but this is an uneasy fit because it is hard to measure and the value of privacy is subjective.

Since its inception, the CCI has had multiple opportunities to examine the digital sector; nonetheless, on 22.01.2021, the CCI published a Market Study on the Telecom Sector in India[2], which highlighted the connection between Data Privacy and the Competition Act. CCI explained data consumption as 'non-price competition' in its Telecom Report, meaning that data gathered from customers by an organization may be used to gain a competitive advantage over its market competitors.

In 2021, the CCI in its *prima facie* order[3] against WhatsApp acknowledged privacy as a non-price parameter of competition, holding that data-sharing between WhatsApp and Facebook amounted to a degradation of quality. The matter was concerned with the WhatsApp's 2021 privacy policy update concerning the sharing of user data on WhatsApp with Facebook. WhatsApp informed the users of the amended policy by sending them prompts asking for their approval by a specific date, failing which the users would be completely barred from using any of WhatsApp's services. The CCI pointed out that the 2021 privacy policy was 'take-it-or-leave-it' in nature because, unlike WhatsApp's earlier policy revisions, it did not provide users with a 'opt-out' alternative. The CCI found that WhatsApp engaged in unreasonable data collection and sharing. The CCI was cautious

[2] https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf
[3] Suo Motu Case No. 01 of 2021 accessed at https://www.cci.gov.in/antitrust/orders/details/100/0

in asserting its power when WhatsApp argued that the claims about data sharing were connected to the Information Technology Act, 2000 and privacy regulations, not being under the jurisdiction of the CCI. CCI contended that excessive data gathering and processing could result in a competitive advantage and possibly have exclusionary implications, bringing the matter inside the purview of the Competition Act.

Here, I would be remiss if I did not mention a significant milestone in India's rapidly evolving technology landscape, namely the enactment of the Digital Personal Data Protection Act, 2023[4] ('DPDP Act'). The DPDP Act's central goal is to increase accountability and responsibility for entities operating in India, such as internet companies, mobile apps, and businesses involved in the collection, storage, and processing of citizens' data. This legislation, with a strong emphasis on the "Right to Privacy," seeks to ensure that these entities operate transparently and are accountable when it comes to handling personal data, thus prioritizing Indian citizens' privacy and data protection rights.

The scope of the DPDP Act extends beyond Indian borders, encompassing digital personal data processing activities conducted outside of India. This extension applies specifically to organizations that sell goods or services to Indian citizens or conduct profiling of Indian citizens. As a result, the Act strengthens data protection measures not only within India, but also with regard to Indian citizens' data handled abroad.

Another feature of the DPDP Act is that before collecting and processing personal data, the DPDP Act mandates that data fiduciaries—such as digital service providers—ask user consent. Personal data is any information that can be used to identify an individual. The DPDP Act does not apply to any personal information that has been made publicly accessible by the data principal (the person whose personal information was gathered). According to the DPDP Act, the data principal is responsible for all consequences if they choose to withdraw their consent. This implies that the services offered by the data fiduciaries may not be available to data principals who have revoked their consent. Additionally, the data fiduciaries are obligated to delete all personal data if the data principle withdraws consent or once the intended use of the data has been realized. In essence,

[4] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

DPDP Act mandates 'free consent' by a data principal before a service provider can process or use user personal data.

The Competition Act and the DPDP Act – two lions maintaining a balance in the jungle of digital era or two friendlies is a question to ponder upon. Two key legal frameworks that cover various aspects of the present digital world is the newly launched DPDP Act and the Competition Act. In contrast to the latter, which focuses on ensuring fair competition and preventing anti-competitive actions in the market, the former prioritizes protecting user privacy and personal data. A balance between data protection and healthy market competitiveness is ensured by the interaction between these two laws, which together form the developing digital ecosystem. We have seen a plethora of pleas taken by the parties before the CCI stating that CCI does not have jurisdiction to try cases where there is a sector specific regulator for instance Copyright Boards, TRAI, *etc*.

Both the DPDP Act and the Competition Act are concerned with the dissemination of personal data to digital players and its legitimate use. It is evident that both the DPDP Act and the Competition Act explicitly address the need for consent for the collection and processing of user data, at least by dominant businesses. The varying goals of the legislation are the root of the conflict between the two. The Competition Act aims to stop dominant businesses from unfairly obtaining consent to gather personal data for their own commercial advantage, whereas the DPDP Act aims to prohibit the exploitation of personal data. While the DPDP Act is clear in its limited purpose of protecting user data, parallel allegations under the Competition Act cannot be ruled out. This creates yet another case of parallel jurisdiction between the DPDP Act and the Competition Act.

As a final observation, I acknowledge the union of DPDP Act and the Competition Act in India not as a clash, but as a harmonious convergence. By fostering collaboration, addressing legal complexities, and embracing the digital era, India can achieve a dynamic legal landscape that propels both creativity and fair play. Mutual co-existence is a must for striking a balance between the two. In fact, the Competition Act has an enabling provision for mutual consultation between authorities. In cases relating to data protection and privacy, the CCI may make reference to the concerned authority to obtain and consider its opinion before issuing an order. Concomitantly, the

authorities established under the DPDP Act may also seek CCI's opinion during the course of their proceedings.

Last but not the least, while we can see the dynamic duo of DPDP Act and Competition Act, the business operating in the digital markets need to go an extra mile for ensuring that their data collection and processing practices are in compliance with applicable data privacy regulations. Consumers on the other hand, should remain informed and choose products/ services offering robust privacy protections. Consumers should be aware of potential anticompetitive action by dominant market participants, as well as understand and exercise their rights to access and control their personal data