Touchstone Partners

GREY MATTERS

The Privacy Conundrum in Antitrust

July 2022

A. Background

The emergence of digital platforms as a part of our daily life and the increasing number of mergers and acquisitions in the technology / digital space have made the interplay between the application of competition and data protection laws more nuanced in the last few years. Whilst the interaction between these two regimes is at a nascent stage at the moment (not just in India but also globally), as this article explains, developments such as the introduction of the Personal Data Protection Bill, 2019 (the ***PDP Bill***) – which is currently pending before the Indian Parliament – and the recognition of privacy as a non-price parameter of competition by the Competition Commission of India (the ***CCI***) as part of a recent market study show that these two regimes may be more inter-related than they may seem at first sight.

Diving into the antitrust issues that entities in the technology / digital space may present and how these may play out in view of the impending data protection regime therefore becomes important. At present, enforcement cases pertaining to big data typically involve exclusionary or exploitative conduct such as self-preferencing / preferential treatment by big tech entities. This could be seen in, for instance, the April 2022 *prima facie* order of the CCI against Zomato and Swiggy whereby the regulator found preferential treatment being accorded on their platforms to restaurants in which they had an equity or revenue interest (amongst others).

On the other hand, in merger cases, issues primarily revolve around accumulation of data by a big tech entity as a result of a merger and the adverse effects on competition as a result of lack of access to such data for competitors / other market players. In its December 2016 order in *Microsoft / LinkedIn*, the European Commission (the ***EC***) observed that the post-merger combination of two datasets may increase a merged entity's market power for the supply of such data or increase barriers to entry for competitors who require such data for their operations. Alternatively, the merger may eliminate competition between two independent entities that were previously competing with

each other on the basis of the data that they controlled.

Since the remedies in such data-intensive cases could well involve the opening up of access to such consumer data to competitors, it is pertinent to examine the impact such remedies could potentially have on consumers from a data privacy perspective, as well as the jurisdictional tussle that may arise between the CCI and the data protection authority that is contemplated to be established pursuant to the PDP Bill.

B. Privacy concerns in data-access related merger remedies

In the recent past, technology-related mergers and acquisitions have been increasingly landing up on the radar of competition regulators around the world. Competition regulators have also largely been cognizant of the increase in innovation and consumer benefits that emerge from such mergers and acquisitions. There have, however, been a few cases requiring remedies involving the grant of access to consumer data post the merger to competitors / other market players to level the playing field.

This was seen in, for instance, the December 2020 order of the EC in *Google / Fitbit*, wherein the EC arrived at the conclusion that whilst the European Union had a data protection regime in place, this regime did not eliminate the possibility of anti-competitive effects due to parties' control on data. In this case, very few market players had access to consumer-related data which was equivalent to that being collected by Fitbit, and Google's acquisition of Fitbit (and its data) was viewed as possibly leading to anti-competitive effects. To address this concern, Google committed to provide access to software applications to certain health and fitness data of users, as offered through Fitbit's web Application Programming Interface, free of charge subject to user consent consistent with applicable laws. However, whether this caveat alone is practically sufficient to safeguard consumers' personal data is arguable.

Whilst a merger remedy involving the grant of access to non-personal data does not appear to be concerning *per se*, cases that involve grant of access to data that is considered by the law (or even by the individuals themselves) as 'sensitive personal data or information' could be tricky. Such a remedy appears kosher from an antitrust perspective as it simply attempts to ensure that data accumulation in a transaction does not lead to any entry barriers or foreclosure concerns and thereby safeguards competition. Could it, however, be that the consumers' right to privacy with respect to their personal data takes a backseat in such cases?

In India, the right to privacy and to safeguard one's 'personal' information is guarded by the Constitution of India and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (which accords protection to sensitive personal data or information). This right is expected to be further strengthened with the enactment of the PDP Bill.

The question that arises therefore is how does a data-access remedy (as imposed by a competition regulator upon merging parties) dovetail with the consumers' right to privacy? Whilst the PDP Bill provides that entities collecting personal data of consumers may process such data (which would include providing

access to the regulators with the relevant data) in compliance with any order or judgment of any court or tribunal in India without obtaining prior consent of the relevant consumer, we do not believe that the intention for such a carve out is to allow sharing of personal data of consumers on a "wholesale" basis pursuant to say an order of the competition regulator. In the absence of adequate safeguards (including consumers' consent), a data-access remedy involving personal data could potentially violate the consumers' right to privacy and also end up diluting one of the primary goals of competition law (i.e. to protect consumers' interests).

C. Potential jurisdictional issues

As mentioned earlier, the CCI has even recognised privacy as a non-price parameter of competition in its January 2021 market study on the telecom sector in India most likely with a view to assert its jurisdiction on privacy issues. Notably, this market study recognises the tension between opening up access to data and protection of consumers' privacy. Further, the CCI has observed that abuse of dominance can take the form of lowering the protection of consumers' privacy, which raises antitrust concerns as a low standard of privacy implies lack of consumer welfare.

With the CCI's March 2021 *prima facie* order in the WhatsApp privacy policy case and the Delhi High Court's decision upholding the investigation, it has become clear that the CCI will continue to exercise its jurisdiction over alleged anti-competitive conduct, even if these overlap with or fall under the larger ambit of privacy-related issues.

Whilst this does not raise concerns of a jurisdictional tussle at present due to the fact that India still does not have a robust data protection authority, it must be kept in mind that the PDP Bill seeks to remedy this gap by establishing an independent data protection authority which will have extensive powers including conducting inquiries and taking action in case of breach of personal data including imposing any penalties. Accordingly, it remains to be seen once the PDP Bill becomes law as to whether the competition and data protection regulators are able to function without any jurisdictional issues coming in the way such as was the case with the Telecom Regulatory Authority of India.

This also begs the question as to whether the above situation could possibly be exacerbated by the CCI, using its first mover advantage, getting involved in other privacy-related cases (if any) till the time the data protection authority is set up? Whilst only time will tell, given the significant overlaps, the expectation is for the CCI and the data protection authority to work together without necessarily encroaching on each other's scope.

D. Conclusion

The interplay between competition and data protection laws needs to be studied in greater detail, especially the effects of different remedies (that may be imposed in data-intensive mergers) on consumers and their right to privacy.

Where the grant of access to data – particularly involving consumers' personal information – to competitors / other market players is permitted,

query whether this could be done in an aggregated and anonymised manner to ensure protection of consumers' right to privacy (although the risk of such information being disaggregated and deanonymised does remain). Moreover, remedies in data-driven merger cases could be finalised by the CCI and the merging parties in consultation with the data protection authority (once established), to the extent necessary. Inter-regulatory coordination would, accordingly, be paramount.

For further information, please contact:

Gaurav Desai
Partner
gaurav.desai@touchstonepartners.com

Anuj Bhatia
Partner
anuj.bhatia@touchstonepartners.com

Shruti Bhat
Senior Associate
shruti.bhat@touchstonepartners.com

Apurva Badoni
Associate
apurva.badoni@touchstonepartners.com