WHEN COMPANIES CHANGE HANDS, WHO OWNS THE DATA? PRIVACY AND COMPETITION CONCERNS IN M&A TRANSACTIONS

Sneha Goenka, Narsee Monjee Institute of Management Studies

ABSTRACT

The growing importance of personal data in Mergers & Acquisitions (M&A) has raised important concerns over their transfer and utilisation. Although such data is instrumental in the economic valuation asset-related transaction, since it involves individual privacy rights as well as market concentration concerns. This article discusses the regulatory issues associated with data-driven M&A transactions through am overview of the European Union, US and Indian regulations through a comparative study of Facebook/WhatsApp, Google/ Fitbit and Marriott/ Starwood deals. The article reviews some limitations associated with the current approaches to solving data and competition problems in the process of acquisition. First, it discusses the approach of European union toward integrating the data aspects of M&A transactions into the merger review, the approach followed in the US concerning the enforcement of the privacy regulations, and the approach adopted by India to include the deal value thresholds to overcome the loophole concerning acquisitions escaping merger scrutiny. Three main regulatory gaps are identified during the study including the absence of coordinated efforts between the competition and data protection agencies, temporal gap between pre- and post-merger enforcement and lastly the limitations of valuation-based notification thresholds.

Keywords- Mergers and Acquisitions, Competition law, Deal-value threshold, Data-driven acquisition, Personal Data.

INTRODUCTION

Mergers and acquisitions have always been analysed on the basis of the balance sheet, intellectual property register, and market share. In the new digital age, the key asset acquired through the merger is more often intangible and consist of millions of data related to customer activity, their health records, financial history, and geographical location, such information now becomes the main value factor in valuations of the transaction, which may be more valuable than the tangible assets or even income from them. This issue poses a question that has not yet been answered sufficiently by the corporate law and antitrust legislation: who is the true owner of data owned by the company, and on what conditions can these data be transferred to another entity?

The issue lies at the cross-section of two regulatory schemes, which have evolved largely independently of each other the field data protection law, which protects the individual's interest in his/her personal data, and competition law, which regulates concentrations of market power. It has been increasingly realised that a transaction can very well comply with the rules governing mergers while posing significant risks under the data protection law, or vice-a-versa. The acquisition of WhatsApp by Facebook, Fitbit by Google and Starwood by Marriott, among others are examples of the kind of dangers posed by the transfer of a data-rich target, whose risks become clear much later down the line.[1][2][3] This article tries to examine the legal challenges in considering data as an asset in M&A transactions and transferring the same, further the article tries to identify gaps in the existing regulatory framework and further providing a comparative analysis in the approaches adopted by US and other jurisdictions.

DATA AS AN M&A ASSET

The first thing to address is conceptual and lies in the nature of personal data, which does not fit easily into the concept of 'property' that M&A deals are based on, according to General Data Protection Regulations (GDPR), an entity that process the personal data is called a controller, required to process the data only for specific, lawful purposes and on lawful basis. [4]Thus, the purchase of shares does not imply changing the controller, the corporate entity is

[1] Facebook/WhatsApp, Case M.7217, Commission Decision (Oct. 3, 2014).
[2] Google/Fitbit, Case M.9660, Commission Decision (Dec. 17, 2020).
[3] Information Comm'r's Off., Monetary Penalty Notice: Marriott Int'l Ltd. (Oct. 30, 2020), https://ico.org.uk/media2/migrated/2618524/marriott-international-inc-mpn-20201030.pdf.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 6(4) 2016 O.J. (L 119) 1.

simply changing hands and the data processing obligation remains intact. However, an asset purchase or a business transfer, normally, imply the transfer of the personal data to a new controller, and thus the question appears whether the lawful purpose and basis of the processing remain the same after the transfer. Indeed, this issue is directly addressed by the United Kingdom Information Commissioner's Office (ICO) in its data sharing code of practice. It states that where a merger or acquisition requires the transfer of personal data to a different or additional controller, the parties should treat data sharing exercise as a part of due diligence, establish lawful basis evaluation, and transparency to the data subjects.[5] Further the issue comes from article 6(4) of GDPR that allows the controller to process the personal data for the purposes, defined in terms of the relationship between the purposes, context of the data collection and expectations of the data subjects. In cases when an acquirer plans to use the personal data of the customers of the target company for any other purposes than the purpose of original business (for example, cross-selling the products that the target company did not sell before), this compatibility condition not just the transfer of the property itself, is what matters most, but is often ignored.

Secondly, the practice of due diligence has not been able to meet up with expectations in terms of regulatory compliance. For instance, the penalty imposed by the ICO on Marriott international in 219 for the sum of £99.2 million (the final penalty was reduced to £18.4 million in 2020) for the data breach that occurred at its Starwood hotels subsidiary. This happened after the takeover by Marriott international in 2016. It should be noted that the data breach had started much earlier than the acquisition but was uncovered later on.[6] As per the findings of the ICO, failure of the acquirer to do a thorough check of data protection on a target in terms of security architecture as well as the ownership of data is considered a post-acquisition compliance issue for the acquirer.

Third and the most pressing issue in relation to digital markets, is that the loopholes of 'killer acquisition's driven by data has allowed such mergers to slip through entirely undetected by merger control systems around the world. Antitrust regimes typically require the mandatory notification of mergers, acquisitions, joint ventures and other concentrations of business depending on the parties turnover or asset value. In the case of a cash-heavy acquirer acquiring

[5] Information Comm'r's Off., Due Diligence When Sharing Data Following Mergers and Acquisitions (Data Sharing Code of Practice https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/datasharing-a-code-of-practice/due-diligence/.
[6] Information Comm'r's Off., supra note 3.

a young start-up company with little turnover but much data, this would escape antitrust scrutiny altogether on account of being below notification thresholds in spite of conferring great future market power through the data. The case of Facebook's 2014 acquisition of WhatsApp worth approximately USD 19 billion serves as the classic example: the merger was approved by the European Commission under the EU merger regulation on the basis of limitedservice overlaps between the two parties, but without thorough examination of how their aggregated user data might create competitive issues.[7] The dangers of such an approach were made clear later in 2016 (even though the commission has conducted even if assessment assuming user matching was possible) when WhatsApp changed its terms of service to allow phone numbers of the users to be associated with their Facebook profiles for purposes of advertising, which Facebook claimed did not happen, further fined for providing inaccurate or misleading information during the process of a merger in violation of Article 14(1) of the EU merger regulation.[8]

REGULATORY APPROACH OF DATA DRIVEN M&A IN DIFFERENT JURISDICTIONS

In reaction to these loopholes, there have been two types of responses to data from the EU authorities.

First, in a substantive sense, merger control has started to take into account the issue of data concentrations in a concrete way. For instance, in the Google Fitbit case, the European Commission undertook a detailed investigation in Phase II because it suspected that the integration of the wearable health data of Fitbit with the data base of Google for its advertisement business might reinforce the dominance of Google and stifle competition in the emerging market of digital health and wearables. [9]Clearance was accompanied by commitments restricting Google's use of specified health and fitness data for advertising, maintaining third-party access to relevant Fitbit data through the WebAPI subject to user consent, and preserving interoperability between competing wearable devices android.[10]

[7] Facebook/WhatsApp, supra note 1.
[8] European Comm'n, Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information About WhatsApp Takeover, Press Release IP/17/1369 (May 18, 2017), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_17_1369/IP_17_1369_EN.pdf.
[9] Google/Fitbit, supra note 2.
[10] Google/Fitbit, Case M.9660, Commission Decision (Dec. 17, 2020).

Unlike Europe, the US has taken a more consumer protection-enforcement approach toward ensuring compliance with the promised privacy policies as opposed to merger control. This is exemplified by the Federal Trade Commission's lawsuit in 2000 against Toysmart.com, in the case of the insolvent online retailing company owned in majority by Walt Disney, a bid by the company to sell its customer list (with personal data of children) as an individual bankruptcy asset was challenged by the FTC as an unfair or deceptive act under section 5 of the FTC act[11] due to the company's own privacy policy that had promised not to disclose any customer information to third parties. The result of this case was a settlement allowing only on condition that it was for the whole business and not just the data, the buyer was involved in a related market and adhered to the initial privacy policy, despite objections from forty plus state attorney general, the bankruptcy court refused to allow the deal and the Toysmart doctrine is now used in the US as a basis of data transfer in distress M&A.[12] Besides, the FTC initiated parallel litigation for violation of the Children's Online Privacy Protection Act.[13]

India provides one of the newest and potentially most direct legislative solutions to the 'killer acquisition' loophole. In particular, section 5 of the Competition Act, 2002 was amended by the Competition (Amendment) Act, 2023, introducing the deal value threshold whereby any combination exceeding INR 2,000 crore (approximately $240 million) must be submitted to the competition commission of India in case the target of the acquisition has substantial business operations in India, regardless of the meeting of the traditional asset and turnover thresholds.[14] The threshold was notified on 10th September 2024 together with the CCI (Combination) Regulations 2024 and was expressly created in order to address acquisitions akin to Facebook and WhatsApp case, due to their nature they did not meet either the asset or the turnover threshold while still having substantial strategic importance for the merging parties through the ownership data. [15]It is believed that this is a cautious mov which does not shift the burden of proof to the merging parties, and its true strength will show when the CCI starts applying.

With respect to data protection, India's Digital Personal Data Protection Act, 2023 is much

[11] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2018).
[12] In re Toysmart.com, LLC, No. 00-13995-CJK (Bankr. D. Mass. 2000); see also Fed. Trade Comm'n, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000).
[13] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018).
[14] Competition (Amendment) Act, 2023, No. 9 of 2023, § 5(d) (India).
[15] Competition (Minimum Value of Assets or Turnover) Rules, 2024, G.S.R. 547(E) (Sept. 9, 2024).
[16] Digital Personal Data Protection Bill, 2022, § 8(8)(b) (India).

more restricted when compared with the draft bill in 2022. Under section 8(8)(b) of the draft bill of 2022 contained provisions granting general 'deemed consent' for processing of personal data with regard to mergers and acquisitions.[16]

STRUCTURAL GAPS IN EXISTING FRAMEWORK

Three common weakness can be identified across all three regimes.

Firstly, none of the regimes studied has successfully merged privacy and competition analysis in one regulatory process, while the EU regime seems to go furthest in incorporating data considerations in its merger remedies, competition agency has better expertise in assessing the problem of market foreclosure rather than data subject harms (vice-a-versa data protection agency has better expertise in dealing with data subject harms, not with market foreclosure). The case of Google and Fitbit is a good example as Google's commitments have been negotiated by the competition director general of the European Commission, not by any data protection authority, despite the warning made by privacy activists regarding the potential problems in the case of the deal, that cannot be solved via competition remedy.[16]

Secondly, timing misalignment issues persist as merger control review takes place ex ante, prior to a transaction, while data protection enforcement (like the case of Marriott) takes place ex post, after harm has occurred, which leaves a structural hole in which flawed data practices are incorporated in the new entity without an opportunity for external oversight.[17]

Thirdly, despite being quite innovative and addressing killer acquisitions, valuation-based thresholds allow determined bidders to avoid meeting the threshold through structuring consideration payments, deferred payments, and minority stakes acquisition, thus rendering the very killer acquisition concern addressed by such threshold ineffective. Also, the competition agencies typically assess the degree of data concentration in the transaction, but do not look into whether the post-merger use of data by the merged company will comply with the original intent of data subjects, which is exclusively covered by the data protection laws.

Conclusion

In the event of corporate acquisitions, data does not only move alongside other assets, but its

[16] Google/Fitbit, supra note 2.
[17] Information Comm'r's Off., supra note 3.

movement and use may impact the data subject's rights while data accumulation can influence the competitive landscape. The foregoing analysis proves that there are provisions in existing legal regimes that consider such risks, but they are addressed separately and at different times.

The European Union has developed the most advanced system of incorporating data issues into mergers review, especially when access to or control of the data influences competition. In the United States, it becomes clear that enforcement of the privacy pledges is critical when data moves along with a distressed or acquired entity. India starts addressing data acquisitions through transactional value-based merger control and the emerging regime of personal data protection. However, the approach remains fragmented since merger authorities only consider competitive implications while data-protection regulation focuses on the legality of the data processing and the rights of the data subjects.

A coordinated regime needs data to be considered as both a competitive resource and a regulated type of personal information. Pre-acquisition data due diligence should include the examination of the type, sensitivity, source and legitimacy of the data acquired while merger review should incorporate data concentration and its competitive importance. Coordination efforts of the competition and data-protection regulatory authorities will ensure that the issues are not analysed separately from each other.

Overall, the issue is not only about who acquires the data, but whether the law allows it to process the data in the way the transaction foresee.