PRIVACY AS A PARAMETER IN ANTITRUST INVESTIGATIONS: A COMPARATIVE CRITICAL APPRAISAL

Arya Kant & Shailja Beria[*]

Consumers today readily divulge their personal data irrespective of the serious concerns regarding privacy. This paper argues for locating privacy as a parameter in Indian competition law for assessing claims of abuse of dominance. Relevant metrics such as maximisation of consumer welfare, data protection, and maintaining openness of markets are analysed in considering whether privacy can be accommodated within the goals of competition law. By showing how privacy is important from both economic and non-economic viewpoints, its relevance in antitrust analysis is sought to be established. This is done by arguing for its relevance in zero-price markets, and in noting the significance of privacy in driving competition for 'free' services. Having established privacy as an anti-trust parameter, this paper proceeds to determine the relationship between privacy and competition, their apparent anti-complementarity and its resolution. Finally, through an analysis of how various developed competition law regimes have incorporated provisions to reflect the nature of digital markets it draws lessons for a similar integration in India.

Table of Contents

I. Introduction *108*
II. Privacy As A Parameter For Competition *110*
A. Privacy As An Economic Factor *111*
B. Privacy As A Non-Economic Factor *114*
III. The Interaction Of Antitrust And Privacy *117*
A. Application Of The Separatist Approach *117*
B. Adoption Of The Integrationist Approach *118*
IV. Resolving The Anti-Complementarity Of Interests *122*
V. Integration Through Data Driven Provisions In Foreign Jurisdictions *125*
A. Germany *125*
B. Japan *126*
VI. Conclusion *127*

[*] 4th-year students at West Bengal National University of Juridical Sciences, Kolkata. The authors are extremely grateful to Ms. Madhavi Singh for her discussions which fuelled their interest in this area. They are also grateful to the Editors of the NUJS Law Review for their constructive feedback and comments on the previous drafts of this article. All errors, if any, are solely attributable to the authors. The authors may be contacted at arya220123@nujs.edu and shailja220109@nujs.edu, respectively, for any feedback or comments.

I. INTRODUCTION

Consumers in digital markets have been repeatedly shown to be concerned about their data privacy.[1] However, notwithstanding the serious concerns about the loss of control over personal data, they are found to be disclosing their information rather generously. This inconsistency in the consumers' attitude and behaviour has been termed the 'privacy paradox'.[2] It has been argued that entities such as Google, Facebook and Apple have consistently engaged in privacy violations without losing substantial market share or facing sanctions.[3] This has often been viewed as the manifestation of the privacy paradox. However, it has only recently been recognised that consumers enjoy little choice in such matters.[4] The relook at privacy violations through the antitrust lens recognises this lack of choice is caused by these entities' dominance in various markets. As a result, privacy and data protection are increasingly forming part of antitrust analyses.

In its preliminary order, in *Updated Terms of Service and Privacy Policy for WhatsApp Users, In re* ('In Re WhatsApp'),[5] the Competition Commission of India ('CCI') noted that in a data-driven ecosystem, the anti-competitive implications of the excessive collection and use of data require anti-trust scrutiny.[6] It noted that such unreasonable collection and sharing in digital markets could potentially lead to exploitative and exclusionary effects by granting competitive advantage to already dominant markets.[7]

Having established WhatsApp's dominant position, the CCI then ascertained competition law concerns pertaining to the harm caused to consumers through the opacity and vagueness of the policy, the absence of informed user consent, the failure to meet legitimate expectations of privacy and quality and the potential competitive advantage gained by such data concentration.[8] Although the CCI, in its analysis, engaged with a range of violations within the intersection of antitrust and privacy, it did not acknowledge limitations of the existing framework to address this increasingly complex intersection.

Any meaningful analysis of the nature and extent of the role that privacy is to play in antitrust investigations requires as its starting point an

---

[1] Jeffrey Prince & Scott Wallsten, *Empirical Evidence of the Value of Privacy*, Vol. 12(8), Journal of European Competition Law & Practice, 649 (2021).

[2] S. Barnes, *A Privacy Paradox: Social Networking in the United States*, Vol. 11(9), First Monday (2011).

[3] Rachel Scheele, *Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice*, Vol. 12(1), Journal of European Competition Law & Practice, 34 (2021).

[4] Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, Vol. 30, Harv. L. Rev. F., 71 (2016).

[5] Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19.

[6] *Id.*, ¶13.

[7] *Id.*

[8] *Id.*, ¶27.

understanding of where privacy could be placed within the broader goals of antitrust. Establishing privacy as an antitrust goal strengthens the case for its integration into antitrust and an analysis of how developed competition law jurisdictions have sought to achieve these goals. Thereafter, this understanding could be applied to the integration of privacy concerns within the antitrust framework in India.

The scope of the paper is limited to theories of harm pertaining to abuse of dominance under §4 of the Competition Act, 2002 ('the 2002 Act') for two reasons. *First*, the abuse of dominance provision under the 2002 Act is similar to the relevant provision under laws of developed antitrust jurisdictions. *Second*, these theories, though a central part of the analysis in the In Re WhatsApp case, have not been explored in Indian competition law jurisprudence and add an element of novelty to this paper.

It must be noted at this stage that India's effects-based approach[9] on abuse of dominance sets a different standard on the reading of intellectual property rights ('IPR') under §4 of the 2002 Act as compared to §3. Unlike §4, §3(5) of the 2002 Act clearly provides for an exception to an individual's IPR.[10] Such carve out recognises the right of any person to impose reasonable and necessary conditions for protecting IP, specifically conferred under certain identified statutes in the context of anticompetitive agreements. Such an exception however does not extend to unilateral conduct, and thus, does not allow exemption from abuse of dominance cases. The same has been recognised by India in its note to the Organisation for Economic Cooperation and Development.[11] In furtherance of the same in 2019, the Competition Law Reforms Committee that the defence may be allowed in cases involving dominant position,[12] citing practice in the EU.[13] The Parliamentary Standing Committee on Finance in its report said in the absence of an explicit defence enshrined in the law, the CCI will not allow any dominant entity to provide for reasonable protection of its IPR, while being investigated for alleged abuse of dominance.

The government however refused to accept the recommendation of Standing Committee to incorporate the IPR defence in provisions that deal with abuse of dominance. While §4A, proposed in the draft amendment Competition Bill, 2020,[14] incorporated protection for holders of IPR, amongst others, in the

---

9 Google LLC v. CCI, 2023 SCC OnLine NCLAT 147.

10 The Competition Act, 2002, §3(5).

11 OECD, *Licensing of IP rights and competition law – Note by India*, June 6, 2019, available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD(2019)4&docLanguage=En (Last visited on September 25, 2023).

12 Competition Law Review Committee, Report of the Competition Law Review Committee, ¶7.6 (July, 2019).

13 The Committee cited the cases of Parke, Davis & Co. v. Probel, Case 24/67 EU:C:1968:1; Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98; Data General Corporation v. Grumman Systems Support Corporation, 761 F. Supp. 185 (D. Mass. 1991).

14 The Competition (Amendment) Bill, 2020, §4A.

cases of abuse of dominance, the recommendation was not incorporated in the Competition Amendment Bill, 2023,[15] passed by the Parliament.

Thus, if an enterprise is found to be dominant pursuant to Explanation (a) to §4(2) and indulged in practices amounting to denial of market access, it is no defence to suggest that such exclusionary conduct is within the scope of their IPR.

While the role of data collection practices as a means of attaining dominance has been adequately explored in Indian jurisprudence, there is relatively less discussion on the abusive nature of these practices from a consumer welfare perspective. Through its focus on abuse of dominance, this paper seeks to provide a theory of privacy harms arising out of such data collection.

Part II discusses data collection and data privacy act as factors in antitrust cases,considering the goals of antitrust. Part III discusses the various approaches taken when integrating privacy concerns into antitrust analysis. Part IV discusses instances involving the apparent non-complementarity of such goals and how this contradiction may be resolved. Part V discusses the data-driven provisions in Germany and Japan drawing lessons for India. Part VI concludes the paper by discussing how data protection would act as a factor in the present abuse of dominance assessment, and how the inquiry may be enhanced through reforms.

Therefore, our thesis statement is that privacy is an antitrust goal across jurisdictions and must, in the future, play a broader role in shaping India's antitrust framework.

II. PRIVACY AS A PARAMETER FOR COMPETITION

The aim of antitrust is the protection of consumers' interests.[16] Under the Chicago School, the consumer welfare standard gained predominance as the means to make antitrust law effective.[17] The neo-Brandeisian school, which is characterised by its renewed focus on anti-competitive market structures which entrench economic and political powers, would be effective only if it enhances consumer welfare in the long run.[18]

---

[15] The Competition (Amendment) Bill 2023.

[16] Pieter Kalbfleisch, *Aiming for Alliance: Competition Law and Consumer Welfare*, Vol. 2(2), Journal of European Competition Law & Practice, 111 (2011); Fédération Internationale de Football Association (FIFA) v. European Commission, Case T-68/08, February 17, 2011, Judgment of the General Court (Seventh Chamber) (2011) ('European Union').

[17] *See* discussion *infra* Part II on "Privacy as a Parameter for Competition"; The Competition Act, 2002, Objectives.

[18] *See* discussion *infra* Part II on "Privacy as a Parameter for Competition"; Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, Vol. 9, J. of Eur. Competition L. & Practice, 131 (2018).

In this part of the paper, we look at data collection and privacy as possible parameters for determining effect on competition. In two-sided markets, where consumers are offered products or services for free and these are monetised through targeted advertising, personal data can be viewed as the currency paid by the consumer in exchange for the free product, or as a dimension of product quality.

This analysis is applied specifically to such multi-sided markets which meet the twin conditions of being zero-price, and using the data collected to service otherwise 'free' content through targeted advertising, primarily social media networks and search engines.[19] This excludes digital platforms such as streaming services which charge a membership price, which forms their primary source of revenue, but also collect and use extensive consumer data, for instance, in their recommendation systems.[20] It also excludes multi-sided platforms following a 'freemium business model' under which the subsidised service is used to market other paid products, provided, the paid products constitute the bulk of their revenues.

First, we look at privacy and big data through an economic lens, finding them equivalent to a currency and having price. *Second*, we look at privacy and big data through a non-economic lens, where we determine effect on competition based on quality instead of price, privacy being one such quality parameter.

A. PRIVACY AS AN ECONOMIC FACTOR

For the application of §4(2)(a) of the 2002 Act,[21] there must be a purchase or sale of goods or service, i.e., an exchange for the consideration. The argument that the provision of services for free by firms in the digital market still constitutes a sale makes little economic sense,[22] raising the question of what serves as consideration for this exchange.

Further, §19(7) lists 'price of goods or service' as a relevant factor in determining a relevant product market.[23] In a two-sided digital market, where products are offered to users for free and monetised through targeted advertising,

---

19 *See*, Samson Y. Esayas, *Competition in (Data) Privacy: 'Zero'-Price Markets, Market Power, and the Role of Competition Law*, Vol. 8(3), Int. Data Privacy Law, 182 (2018); *See also*, OECD, Handbook on Competition Policy in the Digital Age, 2022 1, 35, available at https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digital-age.pdf (Last visited on September 7, 2023) (on kinds of zero-price markets and quality considerations in such markets) ('OECD Handbook').

20 Jon Markman, *Netflix Harnesses Big Data to Profit from Your Tastes*, February 25, 2019, Forbes, available at https://www.forbes.com/sites/jonmarkman/2019/02/25/netflix-harnesses-big-data-to-profit-from-your-tastes/?sh=30e631566fdc (Last visited on September 7, 2023).

21 The Competition Act, 2002, §4(2)(a).

22 Khan, *supra* note 18, at 710; Herbert Hovenkamp, *Antitrust and Information Technologies*, Vol. 68(2), Fl. L. Rev., 425 (2016).

23 The Competition Act, 2002, §19(7).

personal data can be viewed as the currency paid by the user in return for receiving the free product instead of the monetary currency in a sale or a purchase.[24] The 'zero price' value of a free product in such markets is thus only another number.[25]

Germany is the first country to include zero-price markets in the classification of relevant product markets by amending the provisions of its competition legislation to include markets where a product or service was sold for free.[26] In 2022, the European Commission published its draft revision of the market definition notice,[27] revising it for the first time since its adoption in 1997. The revision puts greater emphasis on non-price elements, such as innovation and the availability and quality of goods and services, and provides new guidance in relation to multisided markets and digital ecosystems.[28] The United Kingdom's ('UK') digital competition expert panel too proposes the 'zero price' view in its report on digital competition.[29] The report states that consumers do not completely understand the extent of data collected in return for the services offered.[30] As a result, firms may end up extracting greater value in the form of data while offering consumers the seemingly attractive proposition of accessing free services, yet extracting a much higher price.[31] For instance, one estimate found that if customers enjoyed ownership of their data and were paid for its use, the cost to Facebook and Google could approximately be USD 8 per customer, per year.[32]

Consumers thus may be inclined to choose between services based on their privacy policy in markets where access to service is gained through disclosure of personal data, making 'privacy a competitive edge'.[33] Australia's Competition and Consumer Commission has similarly launched a consultation on whether its competition and consumer law regime is sufficient to address digital

---

[24] David S. Evans, *Antitrust Economics of Free*, Competition Policy International, 13 (2011).

[25] *Id.*

[26] The Germany Act against Restraints of Competition, Bundesgesetzblatt (Federal Law Gazette) I, 2013, 1750, 3245, §18(2a) (2021).

[27] European Commission*, Review of the Commission Notice on the Definition of Relevant Market for the Purposes of Community Competition Law*, available at https://competition-policy.ec.europa.eu/public-consultations/2022-market-definition-notice_en (Last visited September 25, 2023).

[28] Magali Eben, *The Draft Revised Market Definition Notice: The European Commission Brings the Relevant Market Further into the 21st Century*, Kluwer Competition Law Blog, January 26, 2023, available at https://competitionlawblog.kluwercompetitionlaw.com/2023/01/26/the-draft-revised-market-definition-notice-the-european-commission-brings-the-relevant-market-further-into-the-21st-century/ (Last visited September 25, 2023).

[29] Digital Competition Expert Panel, Report of The Digital Competition Expert Panel: Unlocking Digital Competition (March, 2019).

[30] *Id.*, ¶¶1.121-1.123.

[31] *Id.*

[32] The Economist, *Technology Firms are Both the Friend and the Foe of Competition*, November 15, 2018, available at https://www.economist.com/special-report/2018/11/15/technology-firms-are-both-the-friend-and-the-foe-of-competition (Last visited on September 8, 2023).

[33] 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*, Press Release, March 26, 2014, available at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (Last visited on September 24, 2023).

ecosystem concerns and whether it requires to take an expansive approach or form digital platform-specific rules.[34]

The report of the Competition Law Review Committee, 2019, ('the Committee') recommended that data be recognised as a form of consideration in markets where users do not pay any monetary consideration for availing the platform's services.[35] The Committee reviewed the price definition under §2(o) of the 2002 Act, finding it to be inclusive, covering non-monetary forms of consideration such as data.[36] Notably, the report also recognised that consideration may in effect relate to something other than what it appear to relate to, in the case of data collection the former would be its use in targeted advertising while purporting to be for the improvement of services.

In *Matrimony.com Ltd.* v. *Google LLC* ('Matrimony'),[37] Google raised a contention that online search did not involve any purchase or sale owing to the free nature of services offered. The CCI dismissed this contention, by holding that the revenue earned by this data on the advertising end meant that online search services were not offered for free.[38] However, despite its recognition of the loss of user control over data as a hidden cost of the free services offered in digital markets, the CCI did not explicitly identify the data itself as the cost extracted for these services, but based its analysis on the value extracted by firms on account of this data.

More recently, the CCI in In Re WhatsApp, despite its analysis of WhatsApp's updated terms as an imposition of an unfair or discriminatory condition under §4(2)(a)(i), did not interpret this manipulation of price, in the form of data, as imposition of an unfair or discriminatory price under §4(2)(a)(ii) of the Act.[39] Therefore, despite the report's recognition of price under §2(o), to include data, the CCI does not take this approach in adjudging anti-competitive abuse.

In order to shift from this analysis to that of data as price, particularly excessive price, it is first and foremost necessary to measure personal data in monetary terms. While there exist methods for measuring data in such terms,[40] these must account for differences with actual currency, including the significance

---

[34] Kyriakos Fountoukakos et al., *Competition in Digital Markets: Global Overview*, LEXOLOGY, August 18, 2023, available at https://www.lexology.com/library/detail.aspx?g=bc4ea0a2-393b-4ac4-942e-aac3f1fada45 (Last visited on September 24, 2023).

[35] COMPETITION LAW REVIEW COMMITTEE, *supra* note 12, at ¶2.1.

[36] *Id.*, ¶2.2.

[37] 2018 SCC OnLine CCI 1.

[38] *Id.*, ¶85.

[39] Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19¶30.

[40] Gianclaudio Malgieri & B. Custers, *Pricing Privacy – the Right to Know the Value of Your Personal Data* Vol. 34, COMP. L. & SECURITY REV., 296 (2018); OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers No. 220 (April 2, 2013).

of individual preferences, the lack of scarcity of data, and the immeasurable quality of privacy as a fundamental right which needs to be protected.

B. PRIVACY AS A NON-ECONOMIC FACTOR

When a product or service is offered for free, quality becomes an integral dimension of competition.[41] In such two-sided competitive markets, the firm earns profits not from the consumers of the free service, but from the other side, such as selling consumers' data for targeted advertising in case of digital markets. Such a firm may be incentivised to reduce their product quality on the free side of the market to attain maximum profits. In fact, an analogy has been drawn between the abusive practice of unilaterally raising price, to the unilateral degradation of quality in terms of privacy, data collection, or advertising in a zero-price, multi-sided market.[42] Here, the customer is a commodity traded to the opposite side of the market rather than just the beneficiary of a free product or service.[43]

When a service or product is offered without charge to consumers, the emphasis switches to the value created on the other side of the market. Therefore, firms may prioritise the latter if lowering the quality of the free product maximises profit.[44] The extent to which quality may be degraded depends on the level of competition and the ability of consumers to identify and appraise changes in quality.

This takes particular significance in the case of privacy, for the following reasons. *First*, the existence of the privacy paradox means that there is an inherent irrationality in consumers' behaviour with a strong preference for privacy occurring simultaneously with consumers willingly offering up this data for the use of these services. Therefore, individual preferences may be subordinated to an imposition of Anita Allen's 'unpopular privacy',[45] under antitrust laws.

Second, the strong network effects in digital platforms make it difficult for consumers to opt for alternatives that offer more attractive privacy features. *Finally*, the business models involved depend on advertising as a primary source of revenue. For instance, in 2020, Google generated nearly eighty percent of its

---

[41] Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19¶30; Microsoft/Skype, Eur. Comm'n Case No. COMP/M. 6281, (C7279) (October 7, 2011) (European Commission); Microsoft/Yahoo!, European Commission Case No. COMP/M. 5727, (C 1077) (February 18, 2010) (European Commission); Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimize Quality: A Look at Search Engines*, Vol. 18, Yale J.L. & Tech., 72 (2016).

[42] OECD, *Quality Considerations in Digital Zero-price Markets, Background Note by the Secretariat*, Directorate for Financial and Enterprise Affairs Competition Committee, 14, November 28, 2018, available at https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf (Last visited on September 9, 2023); OECD Handbook, *supra* note 19, at 35.

[43] Stucke & Ezrachi, *supra* note 41, at 73.

[44] *Id*.

[45] *See*, K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, Part L, ¶141 (per Chandrachud, J.).

revenue through its advertising business, which is made more attractive through the option of targeting a particular audience.[46] Here, the lack of competitive pressures translates to little incentive to change opaque privacy policies, especially when degraded quality enhances the platform's ability to generate revenues.[47]

Thus, in a digital market where all competing products or services are priced at zero, the firm would seek to collect the most data possible to attain maximum profit. Online privacy and the ability to browse, read, shop, and think online without being watched has been a consumer concern since the turn of this century.[48] Privacy level thus emerges as an important quality attribute.[49] In such zero-price markets, consumer welfare standard analysis can be effective in comparing competition. Regulators determine competition by considering quality aspects such as the privacy offered to the consumer in these 'free' services.[50]

To put it simply, much like a dominant firm with the greatest market share can manipulate price, a dominant firm in a data-driven market can manipulate data collection, potentially leading to exclusionary or exploitative behaviour, raising anti-competitive concerns.

Data has been recognised to have a potential for competitive advantage in India.[51] Probing into data thus should be essential in competition assessments. However, the 2002 Act lacks data-specific provisions, which have stood as roadblocks for the CCI in certain cases. In *Vinod Kumar Gupta* v. *WhatsApp Inc.*,[52] ('Vinod Kumar Gupta') the CCI observed that the data-sharing terms of the privacy policy relate to sharing of users' WhatsApp account information with Facebook to improve the online advertisement and product experiences available on users' Facebook page. This implies that the combined entity, Facebook-WhatsApp, uses data-driven strategies to improve its competitive position in the advertising mar-

---

[46] Sean Herman, *Should Tech Companies be Paying us for our Data?*, Forbes, October 30, 2020, available at https://www.forbes.com/sites/forbestechcouncil/2020/10/30/should-tech-companies-be-paying-us-for-our-data/?sh=339fcd7e4147 (Last visited on September 8, 2023); *See*, Maurice E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, March 27, 2018, Harvard Business Review, available at https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data (Last visited on September 8, 2023).

[47] Megan Graham & Jennifer Elias, *How Google's $150 Billion Advertising Business Works*, May 18, 2021, CNBC, available at https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html (Last visited on September 9, 2023); OECD, *Quality Considerations in Digital Zero-price Markets, Background Note by the Secretariat*, November 28, 2018, Directorate for Financial and Enterprise Affairs Competition Committee, 13-14, available at https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf (Last visited on September 9, 2023).

[48] Chris Hoofnagle et al., *Privacy and Advertising Mail*, Berkeley Cent. For L. And Tech., 14 (2012).

[49] Stucke & Ezrachi, *supra* note 41, at 70.

[50] Digital Competition Expert Panel, *supra* note 29.

[51] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶¶650–652.

[52] Vinod Kumar Gupta v. WhatsApp Inc., 2017 SCC OnLine CCI 32, ¶15.

ketplaces, raising privacy concerns in the process. Despite this observation, since privacy is not a parameter under the 2002 Act, the CCI concluded that any invasion of privacy is governed by the Information Technology Act, 2000, ('IT Act') rather than the 2002 Act.[53]

Despite the lack of data driven provisions, the CCI has recently taken positive steps in deciding cases dealing with privacy concerns. In Re WhatsApp, the CCI highlighted WhatsApp's latest update to be a 'take it or leave it' privacy policy and that the information sharing stipulations mentioned in the policy warranted investigation. It stated that Meta's concentration of user data through cross-linking of data across its social media platforms for targeted advertising gave it a competitive advantage and raised competition concerns.[54] It further went on to state the impugned conduct of data-sharing by WhatsApp with Facebook amounted to degradation of non-price parameters of competition *viz.* quality which resulted in objective detriment to consumers, without any acceptable justification.[55] Thus, the CCI recognised quality of privacy to be a non-price parameter of competition. Further it held that competitors in the market today also compete on the basis of such non-price parameters and that consumers valued non-price parameters of services such as quality, customer service, innovation, amongst others as equally if not more important as price.[56]

In 2021, the CCI released a report on Market Study on Telecom Sector ('the Telecom Report'),[57] which discussed data privacy and competition. In its conclusion, the Telecom Report recognised privacy as a non-price competitive factor. The CCI's observation in the Telecom Report suggests that a lower privacy standard can "result in exclusionary behaviour and abuse of dominance by the enterprises that utilise consumer data".[58] Thus, abuse of dominance can take the form of lowering the privacy protection and therefore falls within the ambit of antitrust as a low privacy standard implies lack of consumer welfare. Even the European Commission has taken a similar view in recognising privacy as an aspect of quality, which could be regarded as a non-price parameter of competition, as discussed in the Facebook/WhatsApp case.[59]

---

53 *Id.*, ¶17.

54 Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19¶30.

55 *Id.*

56 *Id.*, ¶32.

57 Competition Commission of India, Market Study on the Telecom Sector in India, January 22, 2021, available at https://www.cci.gov.in/economics-research/market-studies/details/20/1 (Last visited August 31, 2022).

58 *Id.*, ¶70.

59 Facebook/ WhatsApp, Eur. Comm'n Case No. COMP/M. 7217 (October 3, 2014) (European Commission).

III. THE INTERACTION OF ANTITRUST AND PRIVACY

Academic and judicial literature on the role of privacy in an antitrust investigation has largely taken two opposing directions, the separatist view, and the integrationist view. This part deals with the manner in which the integrationist view has found acceptance in various jurisdictions. It first examines the position in the EU, which has largely followed the separatist approach. Thereafter, it contrasts the EU position with taken by Germany, which has pursued the integrationist approach most actively.[60] This is viewed in light of India's own shift from a strictly separatist approach, to an integrationist one.

The separatist view is based on a rejection of an intersection between competition law and privacy based on the understanding that each area deals with a distinct legal harm.[61] Data privacy law deals with the effective realisation of individual consumer rights through its focus on reasonable expectations and informed consent of consumers.[62] However, antitrust law is concerned not with individual consumer conduct or expectations but with wider concerns of economic efficiency and consumer welfare in the long run.[63] On the other hand, the integrationist view, proposes the integration of privacy as a non-price factor of quality and in turn consumer welfare.[64] As a result, as long as privacy is viewed as a qualitative factor on which firms compete it would be integrated into the antitrust analysis, but privacy on its own would remain outside its purview.[65]

A. APPLICATION OF THE SEPARATIST APPROACH

The European Union ('EU') and its Courts tend to follow the separatist view on the interface between competition and privacy law. The same was established in the cases of *Asnef-Equifax*,[66] and *Google/Doubleclick*,[67] where the Court of Justice and the European Commission refused to intervene in matters relating to personal data protection, on grounds that these were to be dealt with

---

[60] Arletta Górecka, *Competition Law and Privacy: An Opinion on The Future of a Complicated Relationship*, Kluwer Competition Law Blog, June 8, 2022, available at http://competitionlawblog.kluwercompetitionlaw.com/2022/06/08/competition-law-and-privacy-an-opinion-on-the-future-of-a-complicated-relationship/#_ftnref2 (Last visited September 26, 2022).

[61] Erika Douglas, *The New Antitrust/Data Privacy Law Interface*, The Yale Law Journal Forum, January 18, 2021, available at https://www.yalelawjournal.org/forum/the-new-antitrustdata-privacy-law-interface#_ftnref25 (Last visited September 26, 2022).

[62] Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] To Privacy*, Vol. 80, Antitrust Law Journal, 154 (2015).

[63] *Id.*

[64] Douglas, *supra* note 61.

[65] *Id.*

[66] Asnef-Equifax v. Ausbanc, 7 C-238/05 [2006] ECR I-11125, (Third Chamber of the European Court), ¶63 (European Union).

[67] Google/DoubleClick Eur. Comm'n Case COMP/M.4731 OJ C104/10, March 11, 2008 (European Commission), ¶68.

by the EU Data Protection Directive. More recently, in *Facebook/Whatsapp*,[68] the Commission stated that "any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".[69]

In *Microsoft/LinkedIn* the Commission reiterated its stance stating protecting users' personal data fell under the EU Data Protection Rules.[70] The Commission proceeded to discuss the antitrust issues on the assumption that such data combinations were allowed under the data protection legislation in the first place.[71] However, as discussed in subsequent parts, courts in Germany and France have recently adopted the integrationist approach, applying antitrust laws in instances of violation of privacy and abuse of data collection.[72]

B. ADOPTION OF THE INTEGRATIONIST APPROACH

The leading case that marked adoption of the integrationist approach to the role of data protection in an antitrust investigation was the Bundeskartellamt('BKA') decision on Facebook's exploitative business terms.[73] Notably, the German court, specifically clarified that regulations on data protection do not lead to an automatic suspension of abuse control, as it is applicable to the conduct of dominant entities.[74] This distinction is relevant in light of the contrary view taken by the EU, whereby an analysis of General Data Protection Regulation, 2016, ('GDPR') violations by an antitrust authority may be challenged as exceeding its jurisdictional competence.

The BKA linked the 'imposition of unfair terms and conditions' to data protection law breaches, viewing the infringement of the GDPR as an indicator of abusive conduct by Facebook.[75] Both the BKA, and the Bundesgerichtshof ('BGH'),[76] based their ruling on theories of harm that fit closely into the competition framework, including the restriction of choice available to consumers, high

[68] Facebook/WhatsApp Eur. Comm'n Case No. COMP/M. 7217, October 3, 2014 (European Commission).

[69] *Id.*, ¶164.

[70] Microsoft/LinkedIn, Eur. Comm'n Case No. COMP/M. 8124, December 6, 2012 (European Commission), ¶¶177-178.

[71] *Id.*, ¶179.

[72] Autorité de la concurrence, 'Competition Law and Data', 23–24 (2016); Bundeskartellamt, *Background information on the Bundeskartellamt's Facebook proceeding*, February 15, 2019, available at bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.html?nn=3600108 (Last visited on September 26, 2023).

[73] Facebook, Exploitative business terms pursuant to §19(1) GWB for inadequate data processing, Case B6–22/16, (Bundeskartellamt), (February 6, 2019).

[74] *Id.*

[75] Rachel Steele, *Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice*, Vol. 12(1), Journal of European Competition Law & Practice, 34 (2021).

[76] In the German case, although initially, the Düsseldorf Higher Regional Court, overturned the BKA's decision, on appeal, the BGH affirmed the previous decision.

switching costs, network effects and entry barriers.[77] This would envisage a novel type of anti-competitive conduct in the digital environment, where the collection of personal data is not only the source of market power but also, if unlawful, the means of distorting or abusing it.[78]

Network effects are two folds in digital multi-sided markets. Direct network effects affect the consumers' zero-price side and indirect network effects are that which are reflected on the paying advertisements side.[79] The abuse through such framework was delved into by the CCI in *Matrimony. com* case ('Matrimony') with 'big data' being read as a commodity in two sided markets. When users perform searches on search engines, the platform collects a variety of information, including their IP address, device details, location, operating system information, search date and time, and the specific keyword or phrase used. Search platforms leverage this big data to attract advertisers, target relevant advertisements, and run their search business effectively.[80]

The more users an online zero-price service provider has, the more data it collects. Such massive data collection and processing allows the service provider to tailor its services more precisely, thus, rendering the service more attractive to users. The benefits of network effects for the service provider are however not limited to this. Such data collection also allows the service provider to offer more tailored advertisement spots, attracting more user and thus revenues.[81] The mechanism therefore provides the service provider a significant competitive advantage, give rise to substantial entry barriers for newcomers, limiting them from matching the services on both sides of the market provided by the dominant service provider.[82]

Similarly, by discouraging consumers from changing products, switching costs can make entry into established markets more difficult, and dampen the intensity of competition between incumbents. These switching costs can constitute non-monetary elements as well.[83] Data loss, the duration required

---

[77] Facebook, Exploitative business terms pursuant to §19(1) GWB for inadequate data processing, Case B6–22/16, Bundeskartellamt (February 6, 2019).

[78] Giulia Schneider, *Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt' s Investigation against Facebook*, Vol. 9(4), Journal of European Competition Law & Practice, 216 (2018).

[79] *Id*.

[80] Matrimony.com Ltd. v. Google LLC, 2018 SCC OnLine CCI 1, ¶84.

[81] Inge Graef, *Market Definition and Market Power in Data: The Case of Online Platforms*, Vol. 38(4), WCLER, 474 (2015).

[82] Joseph Farrel & Paul Klemperer, *Coordination and Lock-in: Competition with Switching Costs and Network Effects* in Handbook of industrial organization (Elsevier, 2018).

[83] Shin-Ru Cheng, *Market Power and Switching Costs: An Empirical Study of Online Networking Market*, University of Cincinnati Law Review (2021); OECD, *The Evolving Concept of Market Power in the Digital Economy*, 2022, available at https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf (Last visited on September 26, 2023); *See also* ACCC (2021[12]), The European Commission's decision in the Google Android case (AT.40099), the Italian competition authority's Amazon case, the Korea Fair Trade

for creating a new account or re-entering data, decreased functionality of connected products due to compatibility issues, the necessity to rebuy certain content, and even the time required for adapting to unfamiliar systems are thus some forms of switching costs that create entry barriers and may disincentivise consumers form switching platforms in zero-priced digital markets.[84]

While in Facebook/WhatsApp,[85] the European Commission found privacy to be a qualitative aspect and a non-price parameter in assessing competition, it also noted that issues relating to concentration of data strengthening the dominance of a firm and similar privacy related matters fell within the domain of Data Protection Rules and not competition laws.[86]

In Vinod Kumar Gupta, the CCI held that data collection and privacy were issues under the purview of the IT Act, and did not assess the competitive harms arising from such data collection.[87] Thereafter, in *Harshita Chawla* v. *WhatsApp Inc.*,[88] the CCI held that an investigation would be sought in any scenario where there is a possibility of anti-competitive behaviour.[89] In light of the BKA's consolidation of data protection violations into an independent antitrust analysis, along CCI's own shift to the integrationist approach,[90] in acknowledging the possibility of anticompetitive harms, neither the IT Act, nor a specialised data governing statute, if enacted, would preclude the CCI's jurisdiction over data protection, when causing competitive harms.

As discussed in Part II, data privacy violations are not just exploitative on their own but also relevant from the lens of antitrust. The jurisdictional issues that may arise from this integration may be resolved by an understanding that antitrust provides a means to discipline the abusive conduct of dominant entities, whose act of data collection may be both the source of their power, and the means of distorting or abusing such power.[91]

Four years after the Bundesgerichtshof's decision in 2019, the Court of Justice of the European Union ('CJEU') delivered a precedent in deciding Meta's appeal against the BKA.[92] Interpreting the GDPR and the interplay be-

---

Commission's decision in the Google Android Case (2021-329), the Italian competition authority's Amazon case, and the report of the Japan Fair Trade Commission's Expert Study Group on Data and Competition (JFTC, 2017[70]).

[84] Cheng, *supra* note 83, at 124.

[85] Facebook/WhatsApp Eur. Comm'n, Case No. COMP/M. 7217 (October 3, 2014) (European Commission).

[86] *Id*.

[87] Vinod Kumar Gupta v. WhatsApp Inc., 2017 SCC OnLine CCI 32, ¶17.

[88] Harshita Chawla v. WhatsApp Inc., 2020 SCC OnLine CCI 32.

[89] *Id*., ¶56.

[90] Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19.

[91] Schneider, *supra* note 78, at 216.

[92] Meta Platforms and Others v. Bundeskartellamt, Court of Justice of the European Union, C-252/21.

tween data protection authorities and competition authorities in the EU, the CJEU listed requirement to be considered while dealing with instances of personalised use of consumers' personal data for targeted advertising by social media platforms.[93] In upholding the decision of the BKA, the CJEU clarified that an instance of a competition authority taking cognisance of infringement of privacy *vis-a-vis* finding of an abuse of dominance does not replace or supersede the role of a data protection authority.[94]

Confirming to the standpoint of personal data being a parameter for antitrust concern, the CJEU determined that excluding rules concerning the protection of personal data from the legal framework that competition authorities consider when assessing an abuse of dominant market position would ignore the evolving economic landscape.[95] Such an exclusion could potentially weaken the effectiveness of competition law in the EU.

Acknowledging the risk of overlapping jurisdictions, the CJEU held that where such an instance occurs that the national competition authority needs to delve into matters related to the GDPR, it must consult and seek cooperation from the lead supervisory authority for its own assessment.[96] Where the lead supervisory authority has already taken a decision, the national competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law.[97] The CJEU thus in its judgement carves out the differentiation, allowing the competition authority to draw its own conclusions under the application of competition law, when deciding a case involving privacy and personal data concerns.

With the new Digital Personal Data Protection Act, 2023,('DPDP Act') now in place, the Data Protection Board ('DPB') has been constituted to act as the lead supervisory authority in cases of personal data concerns.[98] The original Personal Data Protection Bill, 2019, expressly mandated that if the suggested Data Protection Authority shares jurisdiction with another regulatory body, it must engage in prior consultation with such regulator before making decisions.[99] The same has not been recognised under the new Act. However, despite the same, the 2002 Act prescribes that the Commission may make a reference to other authorities under whose jurisdiction the implementation of the relevant law may fall,[100] thus falling in line with the CJEU's judgement.

---

93 *Id.*, ¶57.
94 *Id.*, ¶48.
95 *Id.*, ¶51.
96 *Id.*, ¶57.
97 *Id.*, ¶56.
98 The Digital Personal Data Protection Act, 2023, §18.
99 The Personal Data Protection Bill, 2019, Cl. 67.
100 The Competition Act, 2002, §21A.

Both the CJEU and the Supreme Court in In Re Whatsapp have considered access to personal data and its processing as significant parameters of competition in digital markets. Both judgements underscore how a dominant company's failure to obtain consent from users before gathering or handling their personal data can lead to the abuse of its dominant position. Therefore, they highlight the increasing alignment in regulations regarding the overlapping concerns of data privacy and competition.

IV. RESOLVING THE ANTI-COMPLEMENTARITY OF INTERESTS

This part examines and addresses potential instances of non-complementarity between privacy and antitrust concerns. When considering the regimes discussed hereunder, it must be kept in mind that despite similarities, the antitrust framework in India has some substantive differences from the jurisdictions discussed.

Misconduct under §1 and §2 of the Sherman Antitrust Act, 1890, may be subject to a 'rule of reason' standard under which once anti-competitive conduct is found, the defendant is allowed the opportunity to establish a valid business justification which is pro-competitive to protect itself from sanctions.[101]

The Federal Trade Commission ('FTC') has largely shown a reluctance to sanction dominant tech entities on antitrust grounds, basing sanctions on the violation of consumer privacy instead.[102] However, the few cases in which privacy has formed part of the analysis highlight the non-complementary nature of privacy and antitrust, whereby dominant entities invoke privacy as a form of business justification against allegations of anti-competitive practices. For instance, in the *LinkedIn* v. *HiQ* case,[103] LinkedIn blocked HiQ from its servers claiming that by providing updates to employers by scouring people's profiles irrespective of the particular user's privacy setting, HiQ was violating these privacy preferences. Subsequently, the courts restored HiQ's access to the data available on LinkedIn consumer profiles. The injunction found little evidence of any privacy harm and made no mention of the accommodation of consumers' preferences on their data privacy with HiQ access.[104]

---

[101] LePage's Inc. v. 3M, 324 F3d 141, 152 (3rd Cir. 2003) (en banc), cert. denied, 542 U.S. 953 (2004); United States v. Microsoft Corp., 253 F3d 34, 57-58 (DC Cir. 2001).

[102] Press Release, *F.T.C., Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, September 4, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (Last visited on September 26, 2023) ('Google Press Release'); Press Release, *Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, July 24, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (Last visited on September 26, 2023) ('Facebook Press Release').

[103] HiQ Labs v. LinkedIn, 938 F3d 985 (9th Cir. 2019).

[104] *Id*., at 1005.

In a series of cases involving allegations of anti-competitive conduct through disparate treatment by digital platforms such as Facebook, Apple and Google, each of these entities have invoked data privacy as a justification in a similar manner. For instance, when Tile raised allegations of anti-competitive conduct against Apple for keeping the default setting of the placing 'always allow' function as 'off', when the same would be 'on' for Apple's own Find MyApp, Apple justified this conduct as being consistent with its own privacy protections.[105]

When privacy itself is raised as a justification against antitrust concerns there is an apparent conflict. However, the anti-competitive harm in such cases does not arise out of the protection of privacy. Rather, it is a result of the gatekeeper role, or dominance, enjoyed by these entities permitting them to extract concessions, and dictate terms to third parties. In Germany, the FCO identified Facebook's competitive advantage by virtue of its collection and collation of consumer data.[106] However, instead of permitting access to this data to its competitors, it imposed restrictions on Facebook's own data collection practices in the interest of competition. This stemmed from its consideration of both sides in multi-sided markets, ensuring that consumer privacy is not compromised in the interest of antitrust.

The Federal Cartel Office's ('FCO') approach also provides a useful guide to the manner in which such conduct is to be disciplined by assessing privacy harms as contributing to and not conflicting with antitrust harms. Under such an approach, HiQ's access to LinkedIn consumer profiles would remain conditional on their adherence to consumers' preferences. Similarly, disciplining of Apple, Facebook, or Google's disparate treatment of competitors would also take into account their own collection of sensitive information, strengthening, rather than impeding the antitrust analysis.

A similar resolution of this apparent conflict was noticeable in Google's Privacy Sandbox initiative, which aimed to protect privacy online by reducing 'cross-site and cross-app tracking' while keeping content free,[107] but invited complaints of anticompetitive behaviour and regulatory scrutiny by the Competition and Market Authority ('CMA').[108] Subsequently, after consultations

---

105 *Apple Comes out Swinging Against Tile after EU Complaint*, The Verge, May 29, 2020, available at https://www.theverge.com/2020/5/29/21274709/apple-tile-european-commission-eu-complaint-app-store-iphone-response (Last visited on September 26, 2023); *Tile says Apple's Behavior is Anticompetitive and has 'Gotten Worse, not Better'*, Reuters, April 2, 2022, available at https://www.reuters.com/article/us-tech-antitrust-apple-tile/tile-says-apples-behavior-is-anticompetitive-and-has-gotten-worse-not-better-idUSKBN21J72V (Last visited on September 26, 2023).

106 Thomas Thieden & Laura Herzog, *The German Facebook Antitrust Case – A Legal Opera*, February 11, 2021, available at http://competitionlawblog.kluwercompetitionlaw.com/2021/02/11/the-german-facebook-antitrust-case-a-legal-opera/ (Last visited on September 26, 2023).

107 Privacy Sandbox, *The Google Privacy Sandbox*, available at https://privacysandbox.com/intl/en_us/ (Last visited on September 26, 2023).

108 Press Release, CMA to keep 'Close Eye' on Google as it Secures Final Privacy Sandbox Commitments, Competition and Markets Authority, February 11, 2020, available at https://www.

with CMA, Google's commitments to address these competition concerns were accepted by the CMA.[109] Through these commitments, the development of the Privacy Sandbox will now be regulated by the CMA, the UK's antitrust authority in consultation with its national data protection authority, that is the Information Commissioner's Office.[110]

Notably, in India, the Standing Committee on Finance, in its fifty-third report on 'Anti-Competitive Practices by Big Tech Companies', proposes this very approach. It proposes the prohibition of a number of data collection practices of 'Systematically Important Digital Intermediaries' (SIDI) including the use "in competition with business users" of data that is not available publicly provided by users in relation to the relevant core services of the platform.[111]

The justification for this approach may be found in the '*per se* rule'. Under the *per se* rule, price-fixing agreements amongst competitors would be illegal *per se* if they threatened to eliminate price competition regardless of their economic justification or reasonability.[112] This is in contrast to the rule of reason where courts identify and balance the competitive effects and the anti-competitive effects of a challenged measure.

The nature of digital markets, particularly their tendency towards monopoly, justifies the application of the *per se* rule when it comes to assessing anticompetitive harms, particularly of their data collection activities. Further, the harms identified Part II would fall within the ambit of abuse of dominance under §4 of the 2002 Act. Notably, under this provision, once an entity is established as dominant, and the entity is found to be indulging in activities that are mentioned in the said provision, its conduct is found to be *per se* violative.[113]

Therefore, once the privacy harm is conceptualised in the form of the imposition of an unfair or discriminatory price, or condition under §4(2)(a) of the 2002 Act, it would be prohibited under statute, provided it was caused by an entity having a dominant position. The next part discusses how data-driven provisions may support the conceptualisation of such a harm in the case of digital markets.

---

gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments (Last visited on September 26, 2023).

109 Decision to Accept Commitments offered by Google in relation to its Privacy Sandbox Proposals, Case No. 50972, Competition and Markets Authority.

110 Media Nama, *Allyou Need to know about Google's Privacy Sandbox*, August 5, 2022, available at https://www.medianama.com/2022/08/223-google-privacy-sandbox-testing-expansion/#:~:text=March%202021%20saw%20a%20group,targeting%2C'%20the%20petitioners%20argued (Last visited on September 26, 2023).

111 *See*, Standing Committee on Finance, Ministry of Corporate Affairs, Fifty third Report on Anti-Competitive Practices by Big Tech Companies, 34 (December 22, 2022).

112 United States v. Socony-Vacuum Oil Co., 1940 SCC OnLine US SC 86; United States v. Trenton Potteries Co., 1927 SCC OnLine US SC 59.

113 OECD, *Roundtable on Safe Harbours and Legal Presumptions in Competition Law - Note by India*, OECD DAF/COMP/WD(2017)58, ¶24 (December 5, 2017).

V. INTEGRATION THROUGH DATA DRIVEN PROVISIONS IN FOREIGN JURISDICTIONS

The integration of data protection and antitrust may be strengthened through legal provisions tailored to data protection concerns of digital markets. This part examines such provisions within German and Japanese laws. While other jurisdictions seek to adopt non-price qualitative parameters into their abuse of dominance regime, Germany remains the only jurisdiction to have expressly recognised a zero price markets framework in analysis of dominance till date. Further, the CCI's Telecom Report[114] specifically recommends Japan's 'Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc' ('the Guidelines').[115] Moreover, analysing the Japanese Competition law jurisprudence allows for observation of the antritrust-personal data interplay from a non-EU/USA perspective.

A. GERMANY

The German antitrust authorities' disciplining of Facebook, discussed in the previous section, is enabled by certain provisions in the German Act against Restraints of Competition, 1958 – *Gesetzgegen Wettbewebbeschränkunge* ('GWB') – particularly those introduced in 2017.[116]

First, an express recognition under §18(2a) of the GWB, of markets where goods and services are provided free of charge, allowed the BKA to assess the competitive harm caused to consumers of the social network market, and conclude that the terms of use impeded their choice, are unfairly imposed by virtue of its superior bargaining power; thereby constitute an abuse of dominance. *Second*, §18(3a) by delineating the factors to be considered in assessing market position and abuse in multi-sided markets, enabled the BKA and BGH to look at the impact of such practices on each side of the market, both private users and advertising companies. *Third*, by incorporating factors such as network effects, access to data that is relevant for competition, and competitive pressures driven by innovation, into the abuse of dominance framework,[117] it enabled the GWB to analyse entry-barriers created by these factors further strengthening Facebook's dominance and impairing competition.[118] As noted previously, the CCI's integrationist approach

---

[114] Competition Commission of India, *supra* note 57, at ¶71.

[115] Japan Fair Trade Commission, *Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc*,December 17, 2019, available at https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217_DP.html (Last visited on September 26, 2023) ('JFTC Guidelines').

[116] Gesetzgegen Wettbewebbeschränkunge ('Act against Restraints of Competition'), 2013, §18(2a).

[117] Rachel Scheele, *Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice*, Vol. 12(1), Journal of European Competition Law & Practice, 35 (2021).

[118] *Id*., 36.

has largely focused on similar competition harms. However, the absence of provisions tailored to discipline data-driven competition severely limits its analysis.

Several authors have identified Facebook's conduct of de-anonymised surveillance by linking cookies with real-world identities as abusive and monopolistic.[119] The BKA incorporated these criticisms into theories of harm, to discipline this conduct within the antitrust framework. In addition to its analysis of abuse of dominance by the imposition of unfair terms with respect to data privacy, the BKA noted that Facebook's conduct caused foreclosure of competition in the advertising market, by impeding competitors who could not amass similar amounts of data. Therefore, the BKA held that in the area of data collection, Facebook, was required to comply with the law that was applicable in Germany and Europe.

B. JAPAN

The Japanese Guidelines state that any use of personal information, including users' purchase history and location, without their consent would constitute an "abuse of a superior bargaining position", a violation specified under Japan's Anti-Monopoly Act, 1947.[120] The Japan Fair Trade Commission ('JFTC') states the Guidelines are intended to "ensure the transparency and the predictability for digital platform operators by clarifying the concepts of the regulation on abuse of a superior bargaining position about acquiring or using personal information, etc".[121] The Guidelines under note seven, eight and eleven specifically list instances of privacy breaches and abuse of superior bargaining position. It takes the view of data being considered as currency while listing instances that unjustifiably cause disadvantage for the consumers, for example, by providing services in equivalent as consideration.[122] Finally, Japan's integrationist view can be discerned by the JFTC's press release on the Guidelines, where it highlights the necessity to cooperate with the Personal Information Protection Commission to tackle abuse of a superior bargaining position regarding the transactions between digital platform operators and consumers that provide personal information, etc.[123]

It is thus observed that Japan's approach on dealing with the competition-personal data overlap falls in line with the CJEU and In Re Whatsapp and the observations made in Part III. Consequently, regulations pertaining to the safeguarding of personal data must not be excluded from the legal framework that

---

[119] Christophe Samuel Hutchinson, *Potential Abuses of Dominance by Big Tech through their Use of Big Data and AI*, Journal of Antitrust Enforcement (2022).

[120] Japan Act on Prohibition of Private Monopolization and Maintenance of Fair Trade, 1947.

[121] Press Release, *Release of the "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc."*, Japan Fair Trade Commission, December 17, 2019, Point 1, available at https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217_DP.html (Last visited on September 26, 2023).

[122] JFTC Guidelines, *supra* note 115, at Note 7.

[123] *Id.*, Point 3.

a national competition authority considers when evaluating potential abuse of a dominant market position, as has been recognised explicitly by Germany. With the DPDP Act and the DPB now in place, the paper recommends for the adoption of such explicit mandated integrationist approach with underlying principles from the CJEU and the GWB to be followed between the DPB and the CCI.

In the absence of data-driven provisions in the 2002 Act, these provisions present in the laws of other jurisdictions bear importance to India's present or future efforts to reform the antitrust framework. However, when drawing from different competition regimes, it must be kept in mind that despite similarities, the antitrust framework in India has some substantive differences from the jurisdictions discussed. The Indian competition framework bears close resemblance to the law in the EU, including Germany.

VI. CONCLUSION

There remains a lacuna in the present application of data protection to antitrust laws insofar as data has not been explicitly recognised as the consideration for sale or purchase under §4 of the 2002 Act. This gives rise to a need to integrate the CCI's analysis of sale and purchase in the Matrimony case with its analysis of abuse of dominance in In Re WhatsApp as follows.

In multi-sided markets consumers first pay a price to the social network, or online search market in the form of data, and this data is then monetised by the advertising services end of the market by the same entity. This would preclude challenges based on the absence of purchase and sale in cases involving the mere collection of data, at zero price. Further it would enable an analysis of abuse of dominance based solely on expansive data collection, which arguably constitutes monopoly rents, addressing the concern of present data practices being largely shaped by dominance of entities rather than consumer preferences.

Once data is understood as price, an antitrust analysis will not be blinded by the efficiency gains through the non-consensual collection of data but would acknowledge the cost of these so-called efficiencies. The retention of a consumer welfare focus would consequently keep the goals of antitrust balanced against, rather than aligned with the monopolists.

As data protection and antitrust harms are increasingly integrated, a non-recognition of multi-sided markets may lead to a violation of consumer consent on one end, when considering the market in terms its paying side, i.e., app-developers, and a denial of market access on the other end when privacy of non-paying users is safeguarded over the interest in data for competing entities. Therefore, it is imperative to conduct a holistic and complementary analysis of the manner in which data collection practices of dominant entities both violate

consumer privacy and permit them to deny market access to their competitors, along the lines of the BKA case, and the In Re WhatsApp case.

This requires a recognition of multi-sided markets as present in §18(3a) of the GWB, and an acknowledgment of zero-price goods or services like under§18(2a). This would permit antitrust harm to be assessed both in terms of unfair price, and unfair terms and conditions under §4(2)(a) of the 2002 Act. It may be argued that the present framework is sufficient in this regard as the CCI found evidence of harm under §4(2)(a)(i) even under the existing law. However, the CCI's present analysis, though not harmful to an antitrust analysis *per se*, presents a relatively less accurate picture in the case of digital markets, than under the German framework.

Further, considering the advent of the DPDP Act and the DPB, an integrationist framework between the CCI and the DPB, as envisaged in the CJEU judgement and the Japanese guidelines need to be put in place for the assessment of anti-competitive harms incorporating instances of privacy violations that would constitute abuse within the Act.

Finally, the present market structure allows the violation of consumer preferences for privacy and data protection, failing the goals of the Chicago school of antitrust, and the broader goals of antitrust. Considering that breaking up these dominant entities may not be viable presently, there is a need to incorporate regulatory structures that protect consumer privacy within the broader antitrust framework. Therefore, privacy as a parameter of consumer welfare is central to the goals of antitrust and must shape India's antitrust framework to effectively address anti-competitive harms.