NLUJ Law Review

Mitali Gupta and Shreya Jha, *The Inclusion of Data Privacy in Antitrust analysis*, 6(2) NLUJ Law Review 1 (2020)

THE INCLUSION OF DATA PRIVACY IN ANTITRUST ANALYSIS

MITALI GUPTA[+] & SHREYA JHA[*]

ABSTRACT

Consumer data is more precious and vulnerable in today's digital economy than ever before. Today, business firms are collecting and storing personal data at a rapid pace with minimal legal safeguards in place. This has implications on both, data privacy policies and antitrust laws. For instance, when data-rich firms such as Microsoft-LinkedIn or Google-DoubleClick, amalgamate, data becomes a primary source of competitive advantage. These scenarios create both data privacy and antitrust concerns. Conflict arises when it is to be determined whether, during mergers, abuse of dominant position coupled with violations of data privacy should be dealt with by competition law or by unique data protection laws. This article seeks to resolve this conflict by first, clearly delineating the goal of an antitrust law and bringing privacy within the scope of antitrust analysis; second, distinguishing those privacy issues which should be addressed by competition law from privacy issues which form a subject matter of data protection law; and third, asserting the need for harmonising the two different-natured legislations of data protection and

[+] The author is a fifth-year student of Amity Law School, Delhi (Guru Gobind Singh, Indraprastha University) and may be contacted at **mitaliminigupta[attherate]gmail[dot]com**.

[*] The author is a fourth-year student of Amity Law School, Delhi (Guru Gobind Singh, Indraprastha University) and may be contacted at **shreya[dot]jha78[attherate]gmail[dot]com.**

antitrust, with the ultimate objective of strengthening user data privacy. In order to achieve the above-mentioned objectives, this article first, describes the digitalisation of economy and privacy issues that stem from it; second, analyses the anti-competitive implications of consumer data; third, explores and analyses the role and need for antitrust analysis in privacy protection; fourth, focuses on the privacy-antitrust conundrum in the Indian competition landscape; and fifth, analyses how privacy can be seen as a competitive advantage with respect to growing awareness among consumers about the vulnerability of their data. Conclusively, this article establishes the protection of data privacy as a role of antitrust law in this digital economy.

TABLE OF CONTENTS

I. INTRODUCTION

The market landscape has drastically changed in the last few decades. The digitalisation of the global economy has set in motion a new wave of capitalism. Markets now operate in a 'digital economy' where the erstwhile relationship between consumers and businesses is transforming significantly.

'Digital economy' is a term used to identify markets where the trade of goods and services are facilitated by digital technologies.[1] One of the characteristic features of this economy is that business models are centred on a flow of 'information' between consumers and business firms.[2] This flow of information largely comprises of the personal data of consumers. In many ways, consumer data has become the 'currency' of this digital economy.

With access to large sets of consumer data and rapidly evolving technology, business firms have started to mine and process this data. Through the analysis that is derived from the processing of personal data, they are able to target goods and services more effectively. They no longer have to depend on the organic chain of demand and supply – they are now capable of creating demand by tapping into the behaviours and buying patterns of consumers.

---

[1] Organisation for Economic Co-operation and Development [OECD], *The Digital Economy*, DAF/COMP (2012)22 (Feb. 7, 2013), https://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf.

[2] Organisation for Economic Co-operation and Development [OECD], *Quality Considerations in Digital Zero-Price Markets-Background Note by Secretariat*, DAF/COMP(2018)14 (Oct. 9, 2018), https://one.oecd.org/document/DAF/COMP (2018)14/en/pdf.

In the hierarchy of things, antitrust laws occupy a significant place in this new age digital economy. When businesses mine and process personal data, two major concerns crop up: *(a)* the privacy and rights of consumers are threatened, and *(b)* a massive divide is created between businesses that can mine consumer data and those that cannot. Since the main goals of antitrust law are freedom of competition, economic efficiency, and protection of consumers and competitors, the regulation of consumer data in this digital economy becomes a concern that falls within the purview of antitrust regulations.

Traditional antitrust analysis, however, concerns itself with 'pricing models' only. 'Pricing models' are various methods that firms use to price their goods and services. Since consumer data is a 'non-pricing model', the traditional antitrust analysis does not take it into account. However, times are changing, and today's digital economy sustains heavily on the personal data of its users. Undoubtedly, there is a strengthened need for the adoption of an approach that goes beyond 'pricing models' to determine the nature and outcome of anti-competitive practices.

When transactions happen in the digital economy, firms tend to collect the personal data of consumers in exchange of services. Usually, this collection happens without the consent or knowledge of users. Data is further compromised when data-rich firms merge or amalgamate, when dominant firms abuse their market power, and when firms resort to unethical practices.

There has been much debate around the inclusion of 'data privacy' as a 'non-price' parameter of assessing competition within the antitrust analysis. The bone of contention is whether privacy breaches emanating from digital transactions warrant examination by antitrust laws or specialised data protection laws.

This article seeks to resolve this debate by analysing the harms of having data privacy 'blind-spots' in antitrust laws. The primary objective of this article is not based upon understanding of how privacy breaches should be tackled, but to analyse the need for the involvement of antitrust regulations in tackling privacy breaches in the digital economy.

II. DATA AND THE DIGITAL ECONOMY

The collection of consumer data in exchange of services is not a novel concept. The practice of collecting personal data by digital forums is not unethical in itself. It does not compromise consumer welfare and is not an anti-competitive practice *per se*.

However, until a few years ago, when firms gathered personal data, they only used it to formulate business strategies or cultivate healthy public relations. There was a difference in the quantity and quality of sensitive personal data collected. Consumers also had more control over the data that they shared.

Today, business firms have unregulated access to large volumes of personal information. They resort to three practices to collect and analyse consumer data—*first*, by directly asking consumers for their data; *second*, by tracking them indirectly; and *third*, by appending other sources of customer

data to their own.[3] Information collected from consumers includes everything from their age, sex, and personality traits, to their sexual orientation, political preferences, and religious beliefs.

Moreover, with the advent of 'Big Data Analytics' and 'data mining', large volumes of unstructured data can be simplified and used to identify and predict patterns and preferences. Personal data now has the potential of being used in machine learning projects and other advanced analytics applications.[4]

'Big Data Analytics' is a process through which computers teach themselves to crunch large datasets. When businesses examine pre-existing databases to generate information which is used to determine the consumer's 'pain-point', it is known as 'data mining'.[5] Big Data Analytics, aided by data mining and deep learning, allows high degrees of permutations and combinations within a data set to obtain desirable results.[6] Through this, businesses can evaluate behavioural patterns of their customers more effectively.

---

[3] Adam C. Uzialko, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESSDAILY.COM, https://www.businessnewsdaily.com/10625-businessescollecting-data.html (Aug. 3, 2018).

[4] *Big data,* SEARCHDATAMANAGEMENT, https://searchdatamanagement.techtarget.com/definition/big-data (last visited Feb. 24, 2020).

[5] Organisation for Economic Co-operation and Development [OECD], *Big Data: Bringing Competition Policy to the Digital Era The Digital Economy*, DAF/COMP/M(2016)14 (Oct. 26, 2016), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M%282016%292/ANN4/FINAL&docLanguage=En [*hereinafter* "**OECD**"]

[6] Emerging Tech from the arXive, *The Big Data Conundrum: How to Define It?*, MIT TECH. REV. (Oct. 3, 2013), https://www.technologyreview.com/s/519851/the-big-dataconundrum-how-to-define-it/.

By simplifying and analysing the data that they collect, firms can design products and services that are tailored to consumer needs.

An example of effective data mining is Walmart Inc.'s identification of the positive association between the occurrence of a hurricane and the consumption of strawberry Pop-Tarts. Walmart recognised that the sale of strawberry Pop-Tarts increased about seven times ahead of a hurricane. Accordingly, it started stocking Pop-Tarts before a hurricane and placed it before the check-out. Soon enough, all Pop-Tarts were sold out.[7]

It is thus evident that new technologies have ushered in a brighter and more efficient market dynamic for big, data-rich business firms. However, it is also evident that consumers pay for this efficiency with their personal, and often sensitive, data.

III. THE ANTI-COMPETITIVE ASPECT OF CONSUMER DATA

While it is widely acknowledged that mining and analysis of consumer data give rise to data privacy concerns, it is also steadily becoming evident that they pose anti-competitive concerns as well. Firms with access to large volumes of consumer data and modern data technologies possess a competitive edge over businesses that do not have access to either of these. This perpetuates an unfair competitive advantage. Violation of data privacy thus needs to be analysed as an antitrust concern. To do this, it is imperative to discuss the implications of privacy breaches on both, consumers and non-dominant market players.

[7] OECD, *supra* note 5.

A. THE IMPACT ON CONSUMERS

The impact of data privacy violations on consumers can be examined via various angles. When assessed through the lens of antitrust analysis, we find it is often argued that violation of data privacy negatively affects 'quality' of services. This argument is founded on the idea that 'privacy protection' must be seen as an aspect of 'quality' of a good or service.[8]

This quality-based approach towards violations of privacy was first articulated by Peter P. Swire, internationally renowned privacy law expert, in his testimony to the Federal Trade Commission[9] during the Google-DoubleClick merger.[10] He argued that 'privacy' must be seen as a component of 'quality' of service, and thus be a part of consumer welfare and antitrust analysis. He also elaborated how violation of privacy is detrimental to the chief goal of antitrust law – consumer welfare.[11]

His approach can be better explained against the backdrop of the Google-DoubleClick merger. Google LLC, he argued, had 'deep' and detailed information about consumer search terms. DoubleClick, on the other hand, had 'broad' information that enabled it to pinpoint surfing

---

[8] KLAUS MATHIS & AVISHALOM TOR, NEW DEVELOPMENTS IN COMPETITION LAW AND ECONOMICS 289 (1st ed. 2019).
[9] Case COMP/M.4731, Google v. DoubleClick, EUR. COMM'N (Mar. 11, 2008).
[10] OLES ANDRIYCHUK, COMPETITION LAW FOR THE DIGITAL ECONOMY 133 (Björn Lundqvist and Michal S. Gal eds., 2019) [*hereinafter* "**ANDRIYCHUK**"].
[11] Peter P. Swire, *Submitted Testimony to the Federal Trade Commission Behavioural Advertising Town Hall* (Oct. 18, 2007), http:/www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire/Testimony_peterswire_en.pdf.

patterns of individuals. After Google's acquisition of DoubleClick, the former acquired both, a deep as well as a broad collection of information.

Before a merger such as this, Swire argued, consumers were tracked by only one database, whereas afterwards, they are subjected to a significantly higher level of tracking.[12] Hence, for consumers with 'high privacy preferences', this amassing of 'deep' and 'broad' information leads to a significant reduction in the quality of the product.[13]

Moreover, when data-rich firms merge, they acquire the power to extract more information from users. This happens not only because the newly amalgamated firm possesses more data, but also because this combined data serves as a tool to profile individuals and invade their privacy.[14] Thus, consumers are likely to experience degradation in the quality of goods and services, especially in post-merger scenarios, as a result of newly acquired market power.[15]

Another example of how data privacy violations can lead to a reduction of consumer welfare can be drawn from Amazon.com, Inc., the leading e-commerce platform. In 2000, Amazon utilised information that it already had to predict the highest prices that American customers would be willing or likely to pay for DVDs. This was termed as 'Price Test'. Although

---

[12] Peter Swire, *Protecting Consumers*: *Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007, 9:00 AM), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/.
[13] Case COMP/M.4731, Google v. DoubleClick, EUR. COMM'N (Mar. 11, 2008).
[14] OECD, *supra* note 5.; MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016).
[15] ANDRIYCHUK, *supra* note 10.

it was eventually discarded due to anger among the customers, it presented one of the earliest instances of how digital platforms may facilitate first-degree price discrimination schemes using aggregated data.[16] Such practices reduce the welfare of consumers in a competitive market.[17]

Consumer welfare is not just compromised when firms actively misuse data but is also compromised when firms collect data without any safety regulations in place. Walmart, for instance, interacts with its consumers through both, 'brick-and-mortar' stores as well as its website and app. It is thus able to collect about two and a half petabytes of unstructured data from its 1 million customers, through which it can extrapolate a consumer's age, gender, parenthood, driver's license number, etc.[18]

Similarly, Uber Technologies, Inc. knows the travel pattern of its customer, through which it may be determined where the customer lives, eats, exercises, etc. Smart speakers, like Amazon Echo or Google Home, which are activated with certain 'wake words', keep their listening device active at all times. This has raised various data security issues, such as the possibility that these devices are constantly listening to and storing private conversations.[19] Further, companies like Facebook, Inc. and Google LLC,

---

[16] Todd. R. Weiss, *Amazon apologizes for price-testing program that angered customers*, COMPUTERWORLD (Sept. 28, 2000, 1:30 PM), https://www.computerworld.com/article/2588337/amazon-apologizes-for-price-testing-program-that-angered-customers.html.

[17] Peter Swire & Lagos Yianni, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2012).

[18] Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L. J. (2018).

[19] Ben Dickson, *Beware the privacy and security risks of smart speakers*, TECHTALKS (June 5, 2018), https://bdtechtalks.com/2018/06/05/google-home-amazon-echo-privacy-security-risks/ [*hereinafter* "**Dickson**"].

collect data from their users and monetise it to target specific consumer groups by selling their advertising spaces.[20]

In what came to be known as the 'Cambridge Analytica Scandal', it was revealed that the company Cambridge Analytica had allegedly mined data of 87 million Facebook users to target campaigns during 2016's US Presidential Election.[21] In his book *People v. Tech*, Jamie Bartlett compared this to the "chipping away of the pillars of democracy and upending of fundamentals of capitalism."[22] Facebook was accused of privacy violations, sharing customer data with Cambridge Analytica, and illegal manipulation of public opinion during the US Presidential Election as well as India's 16th Lok Sabha Elections.[23]

These instances point to the conclusion that user data privacy is vulnerable to breaches in the digital economy and digital democracy. While a lot of this data is collected sans the consent or knowledge of consumers, often consumers are forced to share their data because they have no choice.

---

[20] Marc Israel, *The CMA launches a new market study in a bid to keep pace with a fast-moving digital economy*, WHITE & CASE (July 9, 2019), https://www.whitecase.com/publications/alert/cma-launches-new-market-study-bid-keep-pace-fast-moving-digital-economy.

[21] Charmy Harikrishnan, *Micro targeting of voters can swing entire elections: Bartlett, who discovered Congress poster in Cambridge Analytica office*, ECONOMIC TIMES, https://economictimes.indiatimes.com/news/politics-and-nation/micro-targeting-of-voters-can-swing-entireelections-bartlett-who-tweeted-congress-ca-poster-pic/articleshow/63659215.cms (last updated Apr. 9, 2018, 3:58 PM).

[22] ANDRIYCHUK, *supra* note 10.

[23] Neeraj Chauhan, *CBI begins examining Cambridge Analytica data breach scandal*, TIMES OF INDIA (Aug. 3, 2018, 7:50 PM), https://timesofindia.indiatimes.com/india/cbi-begins-examining-cambridge-analytica-data-breach-scandal/articleshow/ 65261565.cms.

In existing data protection frameworks in India and around the world, firms can invade user privacy as long as they disclose it in their terms and conditions. These terms and conditions are generally bulky, incomprehensible, or ambiguous.[24] Consumers are thus left with no choice, making the so-called concept of 'consent' under data protection laws illusory.[25] The only options available to consumers are either to hand over their data or to avoid digital services altogether.

Besides this, multi-service firms in the online market often collect data for a certain purpose but use it for purposes other than those that consumers consented to. For instance, firms often transfer or sell the data of their users to third-parties that have no direct relationship with these consumers. In a research conducted by Privacy International, it was found that over 60% of Android apps, such as Spotify, Duolingo, Trip Advisor, Period Tracker Clue, etc., shared data with Facebook, regardless of whether or not the user had a Facebook account.[26] Similarly, Bounty, a well-known

---

[24] Hal Singer, *Germany's Antitrust Agency Cracks Down On Facebook: But Is Antitrust The Right Tool For The Job?,* FORBES (Mar. 18, 2019, 6:05 AM), https://www.forbes.com/sites/washingtonbytes/2019/03/18/germanyscompetitionagency-cracksdown-on-facebook-but-is-antitrust-therighttoolforthejob/#7388fe02260e.

[25] Eur. Data Prot. Supervisor, *Privacy and competitiveness in the Age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* EUR. COMM'N (Mar., 2014), https://edps.europa.eu/sites/edp/files/publication/14-0326_competitition_law_big_data_en.pdf.

[26] Lorraine, *Investigating apps that share personal data to Facebook without user content,* RESPONSIBLE DATA (July 16, 2019), https://responsibledata.io/2019/07/16/investigating-apps-that-share-personal-data-to-facebook-without-user-consent.

provider of pregnancy and parenting packages, sold data of 34.4 million users to a third-party firm, Equifax, without informing its customers.[27]

The fundamental goal of antitrust law is to protect consumers from exploitative anti-competitive behaviour and unfair transfer of their wealth to firms with market power.[28] The Indian competition law, in particular, ensures healthy competition in the market by setting 'rules of the game' that protect the competition process itself, rather than competitors in the market. This, in turn, leads to economic efficiency, economic growth, and development of consumer welfare.[29] Thus protecting the interests of consumers by safeguarding their data privacy is essential objective of antitrust laws.

B. THE IMPACT ON NON-DOMINANT MARKET PLAYERS

Along with consumers, non-dominant market players also face multifaceted concerns arising out of data collection and mining. For such firms, it's essentially a non-starter to begin collecting their data.[30] Moreover, when dominant firms analyse and mine consumer data, it tends to take the shape of 'unique' and 'non-replicable' data.[31] Since this unique data is only available to some firms, it becomes an antitrust concern. Besides, antitrust

---

[27] Ben Wolford, *Data sharing and GDPR Compliance: Bounty UK shows what not to do*, GDPR, https://gdpr.eu/data-sharing-bounty-fine/ (last visited Feb. 29, 2020).

[28] Jack Kirkwood, *The Fundamental Goal of Antitrust: Protecting Consumers, Not Increasing Efficiency*, 84 NOTRE DAME L. REV. 191 (2008).

[29] Excel Crop Care Limited v. Competition Commission of India, AIR 2017 SC 2734 (India).

[30] Becky Chao, *Where Does Antitrust Law Fit in When Consumer Privacy Is at Stake?,* PAC. STANDARD (Feb. 28, 2019), https://psmag.com/social-justice/can-antitrust-laws-help-keep-your-data-private.

[31] Jay Modrall, *Antitrust Risks and Big Data*, SSRN PAPERS (June 1, 2017), https://papers.ssrn.com /sol3/papers.cfm?abstract_id=3059598.

authorities are concerned that the need for a large volume or variety of data may result in 'entry barriers' for new entrants and small companies that are unable to collect or buy access to the kind of data that is available to established companies.

Thus, the impact of data collection on non-dominant market players emerge in three scenarios – *first*, during mergers and acquisition; *second*, exclusion of competitors by depriving access to data; and *third*, by exercising market power.

i. Mergers and Acquisitions

Mergers and acquisitions strengthen the dominance of existing market players. When data-rich companies merge, they become 'data richer', and acquire new data sets. This becomes a primary source of a competitive advantage which impacts smaller, non-dominant businesses that do not have equal access to data.

During the Microsoft-LinkedIn merger and the Google-DoubleClick merger, the European Commission (*hereinafter* referred to as "**EC**") and the Federal Trade Commission (*hereinafter* referred to as "**FTC**"), respectively, made a common observation that consumer privacy forms a non-price attribute of competition and it may be adversely affected during a merger.[32]

[32] Dickson, *supra* note 19.

While assessing the Microsoft-LinkedIn merger,[33] the EC noted how the integration of LinkedIn with Outlook.com would lead to a significant expansion of its user database, which could, in turn, negatively affect competition in the market. The EC observed that, as a result of the merger, there would be a two-fold reduction in the choices available to consumers. Firstly, new service providers would struggle to enter the market; and secondly, professional social networks, such as Xing, Viadeo, and GoldenLine, that not only act as competitors but also have better privacy policies, will become marginalised and foreclosed.[34]

An identical consideration arose in the case of UK-Everywhere Everything,[35] where the question that was to be examined was whether the proposed joint venture would lead to the creation of a unique database, which would become an essential input for targeted mobile advertising that no competitor would be able to replicate. Likewise, during the Microsoft-Yahoo! Merger,[36] and the Tomtom-Tele Atlas merger,[37] certain considerations regarding efficiency arose, such as whether the merger would allow the company to perform better because of their newly acquired databases.

---

[33] Press Release, Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions (Dec. 6, 2016) (on file with European Commission), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284.
[34] Case M.8124, Microsoft v. LinkedIn, EUR. COMM'N (Dec. 06, 2016).
[35] Case COMP/M. 6314- Telefónica UK v. Vodafone UK/ Everything Everywhere / JV, EUR. COMM'N (Sept. 4, 2012).
[36] Case COMP/M.5727, Microsoft v. Yahoo! Search Business, EUR. COMM'N (Feb. 2, 2010).
[37] Case COMP/M.4854, TomTom v. Tele Atlas, EUR. COMM'N (Oct. 21, 2008).

The Facebook-WhatsApp merger is also worthy of examination.[38] Before the companies merged, their data was separate and compartmentalised. However, after the merger took place, WhatsApp changed its privacy policy, which allowed it to share the data of its users with Facebook.[39] Interestingly, in the mid-2000s, Facebook, a new social media, differentiated from the then market leader MySpace by publicly pledging to privacy. However, with the demise of other social media platforms and the acquisition of Instagram and WhatsApp, Facebook's competition began to disappear. Thereafter, Facebook revoked its erstwhile privacy policy – which allowed its users to vote in case of any change to the privacy policy – and formulated a new one through which Facebook can track user activity across 8 million-plus websites without any option to opt-out. Even if users choose to leave, they would continue to be subjected to surveillance. All these measures strengthened the dominance of Facebook in the market.[40]

Subsequently, a complaint alleging that Facebook had been carrying 'unfair and deceptive' practices by changing its privacy policies and thereby compromising user data privacy was filed.[41] The EC levied a fine of 110

---

[38] Dickson, *supra* note 19.

[39] Anthony Cuthbertson, *Facebook to merge Instagram, WhatsApp and Messenger,* THE INDEPENDENT (Jan. 25, 2019, 3:39 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-instagram-whatsapp-messenger-merge-explained-a8746551.html

[40] Dina Srinivasan, *Why Privacy is An Antitrust Issue*, NEW YORK TIMES, (May 28, 2019), https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html [*hereinafter* "**Srinivasan**"].

[41] Gaspard Sebag, Aoife White & Stephanie Bodoni, *Facebook fined $122 million over WhatsApp deal for misleading EU,* LIVEMINT (May 18, 2017, 2:54 PM), https://www.live

million Euros on Facebook for providing 'misleading information' about the WhatsApp takeover.[42] It was noted that post-merger, Facebook had changed its privacy policy and this allowed it to draw user data from other platforms like Instagram and WhatsApp and was thereby responsible for misleading the Commission by disclosing inadequate information.

Another interesting aspect of this merger, as noted by the Catalan Competition Authority, was that even though post-merger there was a decrease in the number of users, this would not render WhatsApp as unprofitable. In the absence of price, there is no benchmark which helps in assessing how many users should leave WhatsApp to render it unprofitable or pressurise it into changing its policies. Moreover, advertisements generate enough revenue to cover all such potential losses. Thus, in a digital economy, such data-rich firms are capable of rendering services free of cost.

During such mergers, antitrust authorities engage in a 'harm versus benefit' analysis to decide whether or not the merger should be permitted. Authorities assess the advantages that the new entity would reap because of the new combination of different data sets that it would come to possess. This analysis is done in light of the foreclosure of competition in the market.

mint.com/Companies/ejCEXcPyBP9jS72aIyCreL/Facebook-fined-122-millionoverWhatsAppdeal-for-misleadin.html.

[42] Press Release, Mergers: Commission fines Facebook 110 million Euros for providing misleading information about WhatsApp takeover (May 18, 2017) (on file with European Commission), http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

During the assessment of the Facebook-WhatsApp merger,[43] the EC recognised consumer privacy as potential harm but failed to incorporate it as an essential parameter. It merely observed that any privacy concerns flowing from this merger cannot fall within the purview of EU antitrust laws. This approach, however, warrants re-examination.

When two data-rich companies hold a strong position in the market, their combination might lead to foreclosure of competition. Furthermore, the main 'point of contact' between firms and the government where a combined approach can be fostered is during merger assessments.[44] The question of privacy becomes relevant in such cases because mergers might lead to a gain in market power and this might lead to degradation in privacy. Moreover, as discussed above in the analysis of how privacy violations impact consumers, reduced data protection is closely associated with reduced quality of services.[45]

Thus, even if the inherent nature of antitrust laws and data protection laws are different from each other, privacy protection should not be excluded from the ambit of antitrust analysis. Segregating data privacy from competition law based on their separate nature should not be a viable option.

---

[43] Case COMP/M.7217, Facebook v. WhatsApp, EUR. COMM'N (Oct. 10, 2014).
[44] Srinivasan, *supra* note 40.
[45] *Id.*

ii. Exclusion of Competitors by Depriving Access to Data

When firms become 'data-rich', it is often accompanied by the exclusion of non-dominant market players from the market on account of their inability to access the rich volume of data that dominant firms possess.

According to the EC, when dominant firms refuse to grant access to such data to competitors, it does not *per se* become an anti-competitive practice. However, when the data in question is essential for competitors, refusal by the dominant firm may be viewed as an anti-competitive practice. In such cases, the competitor needs to demonstrate that the data in question is unique and that there are no other means of achieving access to the data that it desires.[46]

Refusal to grant access to data could also attract antitrust action if it is discriminatory.[47] An example may be drawn from the Cegedim case decided by the French Supreme Court.[48] The facts of this case revolve around the firm Cegedim SA which had acquired a dominant position in the market by supplying healthcare software solutions and computer services to pharmacies. On a complaint filed by 'Euris', a company specializing in customer relationship management software (*hereinafter* referred to as "**CRM**"), it was found that while Cegedim sold its CRM medical database to pharmacies that used its own or competing

[46] AUTORITE DE LA CONCURRENCE AND BUNDESKARTELLAMT, *Competition Law and Data*, (May 10, 2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?blob=publicationFile&v=2.

[47] *Id.*

[48] AUTORITÉ DE LA CONCURRENCE, *8 July 2014: Health/Medical information databases*, (July 10, 2014), https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/8-july-2014-health-medical-information-databases.

management software, it denied selling it to pharmaceutical labs intending to use Euris' CRM.[49] Due to this, Euris lost about 70% of its CRM software customers between 2008 and 2012. The French Competition Authority's ("**FCA**") decided to impose a 5.7 million Euro fine on Cegedim on the grounds of it being 'unjustified discriminatory behaviour',[50] and the same was upheld by the French Supreme Court.

Often, dominant firms may have access to such data analytics that they can efficiently analyse the patterns and preferences of their users and subsequently target them with tailored advertising. This ends up providing them with a competitive advantage because competing suppliers cannot match the access to, and analysis of, data that dominant firms are capable of having.[51]

During its decision in the case concerning practices by the France Télécom, SFR, Cegetel, and Bouygues Télécom, the FCA issued an opinion on the issue of cross usage of client databases, i.e., cross-selling and its anti-competitive implications.[52] Bouygues Telecom and SFR, two major players in the French telecom market, launched 'quad-play services.' Given its success, France Telecom-Orange, the principal player in the market, also announced its decision to launch a 'quad-play service.' Accordingly, the

---

[49] Florence Ninane & Patricia Carmona Botana (Allen & Overy LLP), *French Supreme Court confirms discriminatory abuse in market of medical information databases for pharmaceutical companies*, LEXOLOGY (Aug. 21, 2017), https://www.lexology.com/library/detail.aspx?g=84b23a3c-41f1-4f5d-b55f-e8ee48089bb7.

[50] Organisation for Economic Co-operation and Development [OECD], *Considering Non-Price Effects in Merger Control - Background Note by the Secretariat*, DAF/COMP(2018)2 (June 6, 2018), https://one.oecd.org/document/DA F/COMP(2018)2/en/pdf.

[51] *Id.*

[52] Decision No. 04-D-48, French Competition Authority (2004).

FCA opined that cross usage of client database is possible by Orange and this may have foreclosing effects.[53]

iii. Market Power

The control of data with a few dominant firms can also become a source of market power. Two factors determine whether this market power is anticompetitive—(i) the scarcity of data and (ii) the relevance of data to competitive performance.[54] Based on these parameters, whether or not entry barriers exist in the market is decided on a case to case basis.

When the Bazaarvoice-PowerReviews merger[55] was proposed,[56] the Court found that BazaarVoice and PowerReviews were the only significant competitors in the market of rating and review platforms. Thus, this merger was viewed as anti-competitive since it would vest such market power with the newly merged entity that entry barriers would be created for other firms.[57]

---

[53] Diarmuid Ryan & Tom S. Pick (Squire Patton Boggs), *French Competition Authority opinion on database cross-selling*, LEXOLOGY (June 30, 2010), https://www.lexology.com/library/detail.aspx?g=ef5609e3-5729-4620-8f6fbd1b748a1a30.

[54] Case COMP/M.5727, Microsoft v. Yahoo! Search Business, EUR. COMM'N (Feb. 2, 2010).

[55] *Justice Department Files Antitrust Law Suit Against BazaarVoice Inc. Regarding the Company's Acquisition of Power Reviews Inc.*, U.S. DEP'T OF JUSTICE (Jan. 10, 2013), https://www.justice.gov/opa/pr/justice-department-files-antitrust-lawsuit-against-bazaarvoice-inc-regarding-company-s.

[56] United States v. Bazaarvoice, Inc., 13-cv-00133-WHO, N.D. Cal. Civ. R. 1-1, (2014).

[57] Laura Wilkinson & D. Jane Cooper, *DOJ's Successful Challenge Of Bazaarvoice's Acquisition: A Reminder That Consummated Deals Are Not Immune From Section 7 Scrutiny*, CORP. COUNS. BUS. J. (Feb. 20, 2014), https://ccbjournal.com/articles/dojs-successful-challenge-bazaarvoices-acquisition-reminder-consummated-deals-are-no.

IV. TRACING THE LIMITATIONS OF ANTITRUST IN REGULATING DATA PROTECTION

It can be reasonably deduced from the examples discussed hereinabove that the lack of policies addressing data privacy issues within the folds of antitrust law is a growing matter of concern. Without such policies in place, the question of accountability looms large. Who is accountable for the protection of the vast amount of personal data that is stored with firms? How vulnerable are consumers to threats of data breaches, discrimination, information manipulation, etc.?

Privacy, being a non-price effect of competition, is often ambiguous and fact-dependent. It is difficult to quantify the amount of privacy violation that has occurred and the amount of reduction in the quality of services as a result. Further, there is a lack of consensus in defining 'privacy harms' since an antitrust injury might not always transpire out of a merger founded on data monopolisation.[58]

On the other hand, other non-price competition effects, like innovation, may arise due to the availability of new data. This may lead to new and better business models. Thus, innovation in the digital economy may be tarred with the "reduced privacy" epithet if an innovation utilises consumer data. There may be situations where these two non-price effects arise simultaneously during the assessment of agglomeration.[59]

---

[58] Geoffrey A. Manne & R. Ben Sperry, *The Law and Economics of Data and Privacy in the Antitrust Analysis*, SSRN PAPERS (2014), https://papers.ssrn.com/sol3/papers.cfm?abstractid=2418779.

[59] *Id.*

According to a report by the Organisation for Economic Co-operation and Development (*hereinafter* referred to as "**OECD**"), when privacy is considered from the perspective of consumer welfare, it involves an analysis of various behavioural issues.[60] For instance, consumers may either display a lack of ability to monitor whether firms are living up to their data protection commitments, or display "excessive pessimism" concerning the degree of privacy protection which they may extract from firms.[61] It is also a concern that, because of the reasons aforementioned, the inclusion of privacy during merger assessments might lead to 'subjectivity' in the process as there may be different dimensions of consumer preference concerning privacy.[62] Furthermore, blocking a merger on the grounds of privacy protection might not necessarily be effective because data sets can be combined regardless through third-party data brokers.[63] Thus, the inclusion of data privacy within antitrust analysis comes with its challenges and dilemmas.

These dilemmas have been subject to varied considerations by competition authorities in different jurisdictions.

In the European Union (*hereinafter* referred to as "**EU**"), for instance, the antitrust analysis goes beyond pricing-models and takes into account five parameters of competition – price, output, quality, choice, and innovation. The stance of the EU is that the data of customers may often

---

[60] Case COMP/M.5727, Microsoft v. Yahoo! Search Business, EUR. COMM'N (Feb. 2, 2010).
[61] *Id.*
[62] *Id.*
[63] *Id.*

be used by businesses for their ends, and this may result in reduced quality of services offered to consumers. When such reduction is a result of a merger or is rooted in an abuse of dominant position, it falls within the purview of antitrust regulations. The EU relied on non-price parameters in various merger cases such as Microsoft-Skype, Facebook-WhatsApp, and Microsoft-LinkedIn.[64] The EU has also enacted the General Data Protection Regulation (*hereinafter* referred to as "**GDPR**") to secure consumer welfare.

The United States, on the other hand, distinguishes between consumer welfare regulations and antitrust laws. Antitrust regulations are applied judiciously. Unless firms enter into agreements or conduct themselves in any other manner that may restrain or harm competition via price or non-price dimensions, their practices are not considered as antitrust violations. Concerns arising out of privacy violations, deceptive advertisements, and reduction in quality of services are considered to be matters within the purview of consumer protection regulations.[65]

The recent decision by Germany's national competition regulator, Bundeskartellamt, in the Facebook case is an example of how user data privacy can be brought within the ambit of antitrust analysis to ensure consumer welfare. In this case, it was found that user data was flowing from websites to Facebook, even when no Facebook symbol was visible on such

---

[64] Organisation for Economic Co-operation and Development [OECD], *Quality Considerations in Zero Price Economy-Summaries of Contribution*, DAF/COMP/WD(2018)147 (Nov. 28, 2018), https://one.oecd.org/document/DAF/ COMP/WD(2018)147/en/pdf.
[65] *Id.*

a website. Moreover, website operators were found to be using 'Facebook Analytics' to carry out user analytics. The Bundeskartellamt recognised that Facebook was abusing its dominant position. Its behaviour was deemed as exploitative because of how its users lost control of how their data was being used.[66] The Regulator held that Facebook-owned services, like Instagram and WhatsApp, can continue to collect data, subject to the fact that users consent to it. User consent was also made compulsory while collecting data from third party websites and assigning them to a Facebook account.[67]

V. THE INDIAN SCENARIO: THE PRIVACY-ANTITRUST CONUNDRUM

The 'digital economy' phenomenon has arrived in India as well. India has recently witnessed a sharp spike in the number of national and multi-national tech and e-commerce giants in the country. These firms have introduced business models that employ Big Data Analytics and data mining to optimise the experience of users. While this has enhanced convenience and contributed to the ease of doing business, it has also intensified privacy and anti-competitive concerns.

These concerns were recently highlighted in the Indian context when the multinational retail corporation, Walmart, acquired a 77% stake in the Indian e-commerce company, Flipkart Pvt. Ltd. The Confederation of All India Traders raised concerns regarding the data security and privacy

---

[66] *Id.*

[67] *Bundeskartellamt prohibits Facebook from combining user data from different sources*, BUNDESKARTELLAMT (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

of Indian online shoppers since they would now be subject to a cross-border flow after Flipkart relinquishes its data to Walmart post-merger.[68] Although this issue was not raised before the Competition Commission of India (*hereinafter* referred to as "**CCI**"),[69] it did initiate the conversation of whether privacy concerns need to be assessed as antitrust issues in India.

The need for 'data privacy' and the 'right to privacy' are gradually gaining recognition by both, the Indian parliament and the Indian judiciary. In 2018, the Supreme Court of India declared 'privacy' as a Fundamental Right.[70] In December 2019, the Minister of Electronics and Information Technology introduced the Personal Data Protection Bill in the Lok Sabha. The Bill seeks to protect individual personal data by setting up consent as a central requirement for data sharing. It further empowers individuals to obtain, erase, update, or prevent the disclosure of their data. The Bill also proposes to establish a Data Protection Authority which will be entrusted with the tasks of protecting individual interest by preventing misuse of personal data. Further, it provides punishment for the processing or transferring of personal data in violation of the Bill and also punishes the re-identification of personal data without the consent of users.

---

[68] Sameer Ranjan, *With Walmart-Flipkart deal e-commerce sector to witness increase in cross-border data transfer*, YOURSTORY (May 14, 2018), https://yourstory.com/2018/05/walmart-flipkart-deal-indian-ecommerce-sector-witness-increase-cross-border-data-transfer.

[69] *Notice under S. 6(2) of the Competition Act filed by Wal-Mart International Holdings Inc. Combination Registration Number C-2018/05/571*, COMPETITION COMMISSION OF INDIA (Aug. 8, 2018), https://www.cci.gov.in/sites/default/files/Notice_order_document/Walmart%20PDF.pdf.

[70] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

The Competition Commission of India can be instrumental in inculcating this right to data privacy within the folds of antitrust laws. The CCI has, in the past, recognized the concept of 'special responsibility', which is the responsibility of dominant firms to not impair competition in the market.

In the case of *Matrimony.com Ltd. and Ors. v. Google LLC*,[71] the CCI observed how dominant firms have a special responsibility, especially in online marketplaces, to ensure fairness. Although fairness was explained in the context of not restricting competition in the market, it can be given a wider interpretation to include protection of user data privacy and strengthen its internal mechanism to safeguard against breach of personal data.

However, the CCI has shown hesitation on aspects related to the merger of data privacy laws and competition laws. In *Shri Vinod Kumar Gupta v. WhatsApp Inc.*,[72] the CCI observed how any breach of privacy policies under the Information Technology Act, 2000 does not fall under the purview of Competition Act, 2002, thus indicating its reluctance towards merging the two areas. Recently, in July 2019, the CCI announced that it would conduct a market survey to look into digital anti-competitive practices. However, it has made no indication as to whether or not it would

[71] Matrimony.com Ltd. v. Google LLC, 2018 Comp LR 101 (India).
[72] Shri. Vinod Kumar Gupta v. WhatsApp Inc., 2017 Comp LR 495 (India).

include consumer data privacy as one of the parameters to determine competition.[73]

Needless to say, as market dynamics evolve, so must antitrust analysis. There is a need to overhaul the Competition Act, 2002 and re-define what anti-competitive practices should include. The Competition Act is a part of the second-generation economic reform that aimed to provide a comprehensive set of guidelines for the prohibition of horizontal and vertical anti-competitive agreements, the abuse of dominant position, and the regulation of combinations which cause or are likely to cause an appreciable adverse effect on competition.[74]

At present, the Competition Act does not allow for the convergence of competition and privacy. Hence, an amendment in the legislation is strongly suggested for meeting the goal of consumer welfare. There is a need to introduce statutory guidelines that explicitly introduce data privacy and unfair concentration of consumer data as parameters of analysing whether or not a merger would be anti-competitive. Such an amendment, coupled with penal measures to enforce it, would help in safeguarding consumer data and protecting it from misuse.

Moreover, modifications are required in the approach taken by the CCI. When the CCI is to evaluate if an agreement would have an

---

[73] Mihir Dalal, *Internet monopolies: India's trust deficit*, LIVEMINT (July 10, 2019, 11:41 PM), https://www.livemint.com/technology/tech-news/internet-monopolies-india-s-trust-deficit-1562781421036.html.

[74] B.S. Chauhan, *Indian Competition Law: Global Context*, 54(3) J. OF INDIAN L. INST. 315 (July, 2012).

appreciable effect on competition, it should factor in the role that access to personal data plays in creating entry barriers, driving out existing competitors, foreclosing competition, and providing a competitive advantage by empowering data-rich firms to provide improved services to consumers. It should also be careful in approving of combinations concerning data-rich firms since combinations like these have the potential of becoming anti-competitive as discussed.

Even though the harmonisation of these different-natured concerns – of data privacy and competition – has not been the priority of either the CCI or the Supreme Court of India, it is inevitable that they converge sooner or later since 'consumer welfare' continues to be the ultimate objective of both these areas.[75] Without addressing data privacy concerns within the purview of competition law, the goal of consumer welfare cannot be met.

VI. THE ROADMAP OF INCLUDING PRIVACY AS AN ANTITRUST CONCERN

It is undisputed that a healthy, welfare-oriented market requires the existence of free and fair competition. Antitrust policies thus need to ensure that a level-playing field is created for all market players. In furtherance of this goal, we suggest certain approaches that antitrust authorities, as well as business firms, can adopt in order to ensure that consumer welfare and market competition do not suffer.

[75] *Consumer Protection and Competition Policy*, The Eleventh Five Year Plan, (Dec. 24, 2019), http://planningcommission.nic.in/plans/planrel/fiveyr/11th/11_v1/11v1_ch11. pdf.

A. USING PRIVACY AS A COMPETITIVE ADVANTAGE

In his support for the federal privacy legislation, Tim Cook, the CEO of the tech giant Apple Inc., stated that "innovation, breakthrough ideas, and great features can go hand in hand with privacy—and they must."[76] This, we believe, is the kind of approach required to find solutions for the concerns that have been discussed so far.

As has been analysed in the preceding sections, the importance of data privacy and ethics has gained global momentum in recent years. There is increased awareness among consumers regarding the impact of privacy violations and the rights that they have to that effect.[77] Across the globe, consumers are now seeking greater accountability. Thus, it is now time for firms to discard the 'race to the bottom' where they acquire data at the cost of consumer privacy in order to gain market power.

Instead of tech firms fostering a trend of 'race to the bottom' of privacy standards by establishing dominance and lack of choice in terms of data privacy for consumers, a 'race to the top' of privacy standards should be followed. There is a need for dominant firms to attach a sense of 'special responsibility' towards privacy and to view 'privacy' as a competitive advantage.

---

[76] Tim Cook, *You Deserve Privacy Online. Here's How You Could Actually Get It*, TIME (2019), https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/.
[77] Kelly D. Martin, Abhishek Borah & Robert W. Palmatier, *Research: A Strong Privacy Policy Can Save Your Company Millions*, HARV. BUS. REV. (Feb. 15, 2018), https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions.

B. DEMARCATING THE ROLES OF CONSUMER PROTECTION LAWS AND ANTITRUST LAWS

As has been done by countries such as the United States of America, a distinction between privacy-related issues which can be handled by competition law, from privacy-issues which can be addressed by specific data protection law, must be drawn.

Privacy is subjective, contextual, and has commercial value, i.e. consumer data is an important commercial good for digital platforms.[78] Thus, antitrust enforcement may try and ensure that it does not interfere in cases where there is no loss of efficiency arising out of the acquisition of consumer data.[79] In such situations, consumer or data protection laws can offer suitable remedies. Besides this, antitrust laws can focus on broader macroeconomic harms and consumer protection and data privacy laws can restrict themselves to specific contractual bargains.[80]

C. 'COMPARE AND FORGET'

Another approach that may be adopted to address the inclusion of data privacy in competition law could be that of "compare and forget", as was suggested by the Dutch Data Protection Authority. This was suggested in the context of service providers like WhatsApp being allowed short term

[78] Maureen K. Ohlhausen & Alexander P. Okuliar, Competition, *Consumer Protection and The Right Approach to Privacy*, 80 ANTITRUST L. J. 1 (2015).
[79] *Id.*
[80] *Id.*

access to the full address book of a user to help the user identify which of their contacts were already WhatsApp users.[81]

D. OTHER APPROACHES

Authorities may also consider other approaches, such as formulating and implementing strict rules to ensure minimal data retention. They may also enact policies that empower individuals to withdraw their data from databases without threats of surveillance and the like. Furthermore, with regards to issues about subjectivity of privacy concerns of consumers, surveys may be conducted to gauge the importance of privacy protection to the consumers.[82]

VII. CONCLUSION

User data, which is highly treasured by firms, have antitrust implications when the data is used in a manner that violates user privacy or creates entry barriers for non-dominant firms in the market. In light of this concern, this article has demonstrated how the introduction of user data privacy within the ambit of antitrust analysis will strengthen consumer welfare without encroaching upon the aims and objectives of specialised data protection laws.

We have also analysed in this article how certain limitations exist in the pre-existing laws relating to antitrust, consumer protection, and data

---

[81] Case COMP/M.5727, Microsoft v. Yahoo! Search Business, EUR. COMM'N (Feb. 2, 2010).
[82] *Id.*

privacy. Furthermore, it may be difficult for all these fields to converge since 'privacy' is often ambiguous and fact-dependent, thus being subjective. Nevertheless, this obstacle should not stop authorities from pushing for the inclusion of data privacy as a non-price parameter of assessing competition in the market.

This article has also discussed at length how, in the status quo, there is a growing awareness among consumers regarding the vulnerable position of their data and rights. To address this, we have suggested that authorities and firms can make efforts to turn consumer data into a competitive advantage instead of a disadvantage by focusing on privacy-friendly policies.

In conclusion, we believe that until and unless an inclusive and holistic analysis of antitrust and consumer data is done, the free market shall continue to suffer and both, consumers and competitors, will not benefit from the true object of antitrust laws. After all, as was said by Charles James, the eminent antitrust attorney, "the standard formulation on remedy is that it ought to cure past violations and prevent their recurrence since that is what antitrust is all about."