

The logo for Σrsa, featuring a large Greek letter Sigma (Σ) followed by the lowercase letters 'rsa'.

Economic
Research
Southern
Africa

Data as the New Currency? Excessive Data Collection and Leveraging as Non-Price Abuses of Dominance in South Africa's Digital Economy

Policy Paper 60

Shaping digital competition policy and
regulation in South Africa

September 2026

Kuhle Majola | Prof. Tinashe Kondo



ERSA Policy Papers address current issues relevant to South Africa's economic policy discourse. They aim to succinctly frame key policy challenges, explain their relevance and significance, and explore potential pathways forward for policymakers and researchers. The papers are primarily narrative in nature, drawing on existing research and descriptive analysis, and seek to contribute to constructive, informed policy debate.

The views expressed are those of the author(s) and do not necessarily represent those of Economic Research Southern Africa. While every precaution is taken to ensure the accuracy of information, Economic Research Southern Africa shall not be liable to any person for inaccurate information, omissions or opinions contained herein. This paper has been peer reviewed.

Data as the New Currency: Excessive Data Collection and Leveraging as Non-Price Abuse of Dominance in South Africa's Digital Economy

Kuhle Majola¹ and Prof. Tinashe Kondo²

Abstract

The rise of the internet has brought with it significant complexities, even for the economy. Not only do we have physical brick and mortar markets, but we also now have digital markets. Digital markets present a significant challenge to competition law. This is because, for instance, dominant firms can extract significant value from users, not through monetary prices, but via the collection and downstream use of personal data. This notwithstanding, to date, the South African abuse of dominance framework has not yet extended its price-centric and foreclosure-based analytical tools to data as a competitive input, which leaves unresolved the question as to how data-driven harms should be addressed under the existing doctrine. Accordingly, this paper aims at responding to this challenge by considering specifically how excessive data leveraging and excessive data collection as non-price-based abuses of dominance are dealt with under the Competition Act 89 of 1998. Methodologically, the paper analyses the existing framework with respect to abuse of dominance and considers digital relevant proceedings such as market inquiries to determine how data collection and data aggregation have been dealt with by South African competition authorities. More importantly, the paper also draws comparative insights from the Indian and German jurisdictions which serve as a contextual benchmark. As part of its findings, the paper observes that there is currently no need for legislative amendments to accommodate non-price-based harms. Rather, what is needed is an evolution in the interpretive approach. Herein, data is recognised as a non-monetary form of consideration and a strategic competitive input.

Keywords: Abuse of dominance, Competition Act 89 of 1998, Data collection, Data leveraging, Digital markets, Exclusionary abuse, Exploitative abuse, Non-price competition, POPIA, Privacy, Zero-price markets.

JEL classification: K21, L41, L86, D18

¹ Analyst, Competition Commission South Africa; LLB (UWC). Kuhle Majola co-led the investigation into the advertising technology (AdTech) market under the Media and Digital Platforms Market Inquiry (MDPMI) and authored the MDPMI's work on regulating online harms. [Linkedin.com/in/kuhle-majola](https://www.linkedin.com/in/kuhle-majola).

² Associate Professor, Competition Law, Department of Mercantile and Labour Law, University of the Western Cape, B.com Law (Economics), LLB, LLM, LLD (UWC). Tkondo@uwc.ac.za.

EXECUTIVE SUMMARY

The digital economy has fundamentally altered how firms compete and create value. Unlike traditional markets, many digital platforms offer services at a zero monetary price while deriving economic value from the collection, processing, and commercial exploitation of user data. In these markets, personal data functions as a form of non-monetary consideration, enabling firms to monetise users through targeted advertising, analytics, and other data-driven business models. While data-driven innovation has generated significant benefits for consumers and businesses, it has also created new competition concerns. Dominant digital platforms are increasingly able to accumulate vast quantities of personal and behavioural data, strengthening network effects, raising barriers to entry, and entrenching market power. Yet South African competition law remains largely rooted in traditional price-centric theories of harm, creating uncertainty as to how competition authorities should assess anti-competitive conduct where harm arises through data practices rather than monetary pricing.

This paper examines whether excessive data collection and excessive data leveraging can constitute forms of abuse of dominance under the Competition Act 89 of 1998. It further explores whether South Africa's existing legal framework is capable of addressing these emerging harms without legislative amendment. The paper finds that South African competition law is conceptually capable of addressing data-driven abuses of dominance. The Competition Act contains sufficiently broad provisions to accommodate non-price forms of harm, including harms relating to privacy, quality degradation, foreclosure, and market power derived from control over strategic data assets. The challenge lies not in the wording of the legislation but in its interpretation and application.

The paper finds that data-related conduct can generate both exploitative and exclusionary forms of harm. Excessive data collection may be understood as both an exploitative abuse of dominance and an exclusionary abuse of dominance. What is interesting to note is that while exploitative abuses are more visible and dominance in these cases, they are much harder to prove. A better prospect of success can be found by pursuing a case of exclusionary abuse, especially in cases where such a party uses their dominance in one market to leverage their position in an adjacent market, to the exclusion of competitors that do not have access to similar data.

In digital markets where users have limited alternatives, dominant firms may impose extensive or intrusive data collection requirements on a take-it-or-leave-it basis. Such conduct may reduce privacy, undermine user autonomy, and degrade service quality. In these circumstances, excessive data collection functions similarly to excessive pricing because users effectively “pay” for services through the surrender of personal information rather than money. Excessive data leveraging by contrast, may constitute an exclusionary abuse. Through the aggregation and leveraging of data across services, markets, or business units, dominant firms may reinforce existing advantages, strengthen barriers to entry, and extend market power into adjacent markets. While data leveraging may create efficiencies and innovation benefits, it can also distort competition where rivals lack access to comparable datasets or are unable to replicate the resulting competitive advantages.

The paper also finds that competition law and data protection law perform distinct but complementary functions. Compliance with the Protection of Personal Information Act (POPIA) does not necessarily resolve competition concerns arising from data concentration or data-driven market power. Similarly, competition law intervention does not require proof of a data protection violation. Rather, the two frameworks should be viewed as complementary regulatory tools addressing different dimensions of harm. The paper draws comparative lessons from developments in India, where competition authorities have increasingly recognised the relationship between data practices and market power. The Competition Commission of India has demonstrated a willingness to assess excessive data collection and privacy-related concerns within abuse

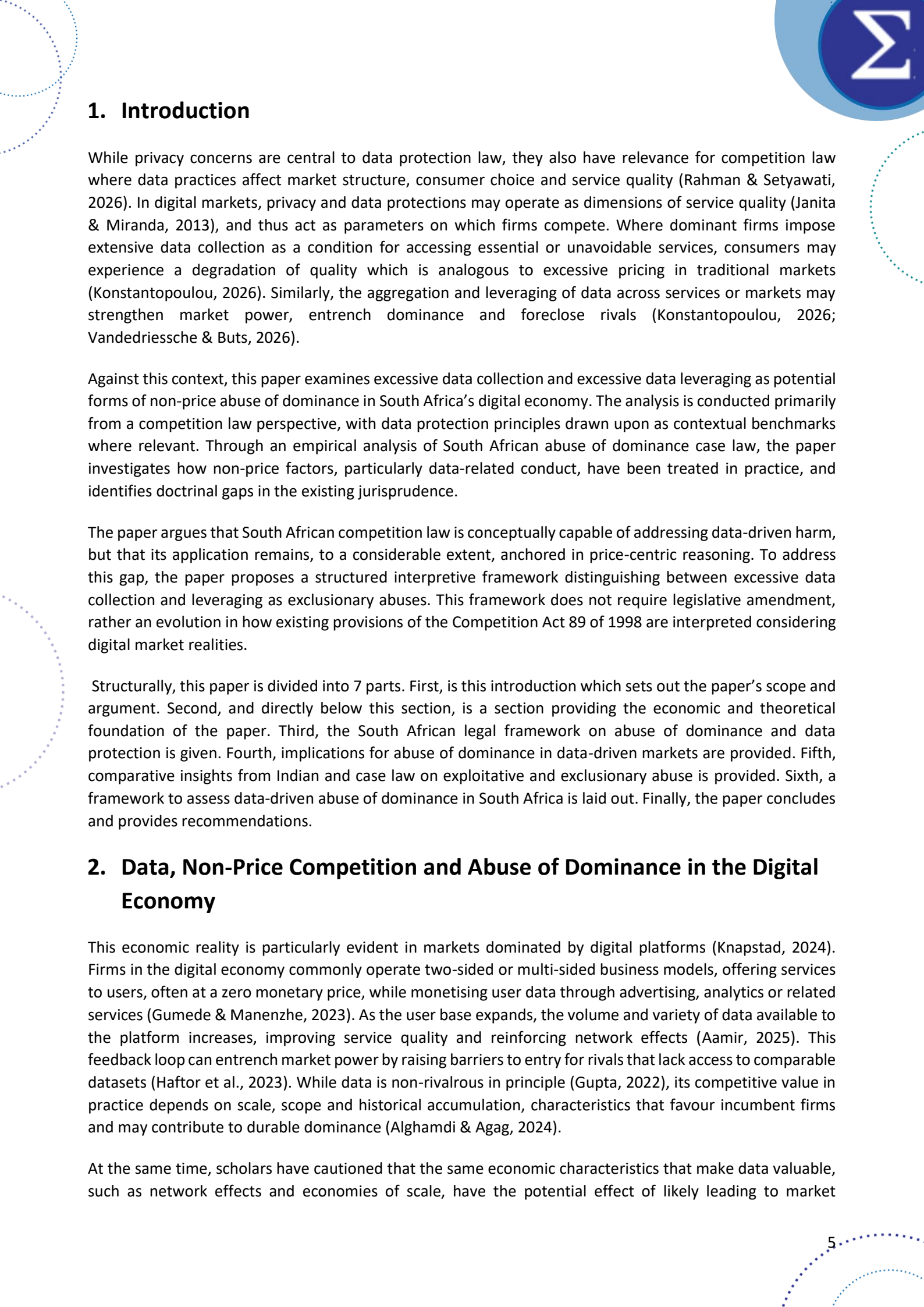
of dominance investigations, particularly in relation to digital platforms. These developments illustrate that competition authorities can address data-driven harms within existing legal frameworks without necessarily requiring new legislation. The Indian experience demonstrates how competition law can evolve to recognise data as a competitive asset and privacy as a relevant parameter of competition.

The paper concludes that legislative reform is not presently required. Instead, South Africa should adopt an interpretive evolution that recognises data as a strategic competitive input and a form of non-monetary consideration in digital markets.

To achieve this objective, the paper proposes a structured framework for assessing data-driven abuses of dominance. Under this framework:

- Excessive data collection should be analysed as a potential exploitative abuse where dominant firms collect data beyond what is reasonably necessary for the provision of a service and where users lack meaningful alternatives. However, because this may be difficult to prove at times, authorities can also pursue this as an exclusionary abuse where the collection of data is utilised to gain advantages in an adjacent market where other competitors do not have access to this data.
- Excessive data leveraging should be analysed as a potential exclusionary abuse where the aggregation, combination or leveraging of data strengthens market power, forecloses rivals, or extends dominance into adjacent markets.
- Competition authorities should incorporate non-price indicators of harm, including privacy, quality degradation, user autonomy, innovation, and data concentration, into abuse of dominance assessments.
- Greater cooperation should be encouraged between competition and data protection regulators while maintaining the distinct objectives and mandates of each regulatory framework.
- Future enforcement should focus on the competitive significance of data rather than limiting analysis to monetary pricing and traditional forms of foreclosure.

As South Africa's digital economy continues to expand, data increasingly functions as a source of economic value, market power, and competitive advantage. The evolution of competition law must therefore reflect the realities of digital markets, where consumers often pay with data rather than money and where anti-competitive harm may arise through reductions in privacy, quality, and consumer choice. This paper demonstrates that the Competition Act already provides a sufficient legal foundation to address such harms. What is required is not legislative amendment, but a broader and more technologically responsive interpretation of abuse of dominance provisions. By recognising excessive data collection and excessive data leveraging as potential forms of non-price abuse, South African competition law can remain effective, relevant, and capable of protecting competition and consumer welfare in the digital age.



1. Introduction

While privacy concerns are central to data protection law, they also have relevance for competition law where data practices affect market structure, consumer choice and service quality (Rahman & Setyawati, 2026). In digital markets, privacy and data protections may operate as dimensions of service quality (Janita & Miranda, 2013), and thus act as parameters on which firms compete. Where dominant firms impose extensive data collection as a condition for accessing essential or unavoidable services, consumers may experience a degradation of quality which is analogous to excessive pricing in traditional markets (Konstantopoulou, 2026). Similarly, the aggregation and leveraging of data across services or markets may strengthen market power, entrench dominance and foreclose rivals (Konstantopoulou, 2026; Vandedriessche & Buts, 2026).

Against this context, this paper examines excessive data collection and excessive data leveraging as potential forms of non-price abuse of dominance in South Africa's digital economy. The analysis is conducted primarily from a competition law perspective, with data protection principles drawn upon as contextual benchmarks where relevant. Through an empirical analysis of South African abuse of dominance case law, the paper investigates how non-price factors, particularly data-related conduct, have been treated in practice, and identifies doctrinal gaps in the existing jurisprudence.

The paper argues that South African competition law is conceptually capable of addressing data-driven harm, but that its application remains, to a considerable extent, anchored in price-centric reasoning. To address this gap, the paper proposes a structured interpretive framework distinguishing between excessive data collection and leveraging as exclusionary abuses. This framework does not require legislative amendment, rather an evolution in how existing provisions of the Competition Act 89 of 1998 are interpreted considering digital market realities.

Structurally, this paper is divided into 7 parts. First, is this introduction which sets out the paper's scope and argument. Second, and directly below this section, is a section providing the economic and theoretical foundation of the paper. Third, the South African legal framework on abuse of dominance and data protection is given. Fourth, implications for abuse of dominance in data-driven markets are provided. Fifth, comparative insights from Indian and case law on exploitative and exclusionary abuse is provided. Sixth, a framework to assess data-driven abuse of dominance in South Africa is laid out. Finally, the paper concludes and provides recommendations.

2. Data, Non-Price Competition and Abuse of Dominance in the Digital Economy

This economic reality is particularly evident in markets dominated by digital platforms (Knapstad, 2024). Firms in the digital economy commonly operate two-sided or multi-sided business models, offering services to users, often at a zero monetary price, while monetising user data through advertising, analytics or related services (Gumede & Manenzhe, 2023). As the user base expands, the volume and variety of data available to the platform increases, improving service quality and reinforcing network effects (Aamir, 2025). This feedback loop can entrench market power by raising barriers to entry for rivals that lack access to comparable datasets (Haftor et al., 2023). While data is non-rivalrous in principle (Gupta, 2022), its competitive value in practice depends on scale, scope and historical accumulation, characteristics that favour incumbent firms and may contribute to durable dominance (Alghamdi & Agag, 2024).

At the same time, scholars have cautioned that the same economic characteristics that make data valuable, such as network effects and economies of scale, have the potential effect of likely leading to market

concentration (Competition Commission of South Africa, 2021). High switching costs and user lock-in can limit the ability of consumers to discipline dominant firms, enabling incumbents to entrench their positions or expand into adjacent markets (Li & Cauffman, 2025). Therefore, data occupies a contradictory position in the digital economy, that is, while it stimulates innovation and efficiency, it also facilitates the exercise and extension of market power (Centre for Internet and Digital Economy, 2026).

Although the dynamics are ambivalent, they have important implications for competition law analysis. Traditionally, competition law has been anchored on price-based indicators of harm, such as excessive pricing or predatory pricing (Competition Commission of South Africa v Media 24, 2019). However, this approach is increasingly unsuited to digital markets in which services are frequently offered at zero monetary prices (Knapstad, 2024). In such markets, competition occurs on non-price parameters, including quality, choice, innovation and the terms on which data is collected and used (Esayas, 2018). Herein, users do not pay with money, they instead “pay” with personal or behavioural data, rendering data practices a form of non-monetary consideration (Just, 2026).

When data is recognised as a non-price parameter of competition, competition law can engage with harm that manifests through the degradation of service quality rather than through higher prices (Crowell, 2026). From a consumer perspective, the demand for increasingly extensive or intrusive data collection may constitute a reduction in privacy as a quality factor, (Esayas, 2017) even where the service remains nominally free. On the other hand, from a market perspective, data practices may distort competition by reinforcing dominance or excluding rivals, independent of any price effects (Competition Commission of South Africa, 2021). Notably, this reframing does not require a departure from established competition law principles but rather reconsidering their application to new forms of consideration and harm.

Within this framework, it is analytically useful to distinguish between excessive data collection and excessive data leveraging, as these practices give rise to distinct forms of competitive harms. Excessive data collection can be appraised as a form of the more traditional excessive prices theory of harm, accepting the analogy data as “the currency of the digital age” (Robertson, 2020). What constitutes excessive can be informed by parameters such as users' reasonable expectations, the parties' bargaining power, principles of proportionality and equity, or the indispensability of a trading condition (Abate et al., 2024). Excessive data collection refers to the extraction of personal or behavioural data from users in quantities or forms that exceed what is reasonably necessary in exchange for the provision of a service (Abate et al., 2024).

In markets characterised by dominance and limited user choice, such practices may be imposed on a take-it-or-leave-it condition (Abraham, 2025), leaving users with little meaningful control over the extent of data surrendered. The result of this is harm which is primarily user-facing, manifesting as degraded privacy, reduced autonomy, and a degradation in service quality (Abate et al., 2024). From a competition law perspective, excessive data collection may therefore resemble exploitative conduct, particularly where users are unable to switch to alternative providers (Abate et al., 2024).

By contrast, excessive data leveraging (this is sometimes referred to by other sources as excessive data sharing, however for the purposes of this paper, this language is mostly avoided as it could be confused with information exchange between competitors) concerns the downstream use of collected data. This includes the internal combination of data across services or markets, as well as leveraging data with third parties for commercial purposes. While leveraging data may promote innovation and efficiency in some circumstances (OECD, 2024), it also has exclusionary effects where it reinforces data advantages that rivals cannot replicate (Kathuria & Globocnik, 2019). The aggregation of data from multiple sources may enable dominant firms to leverage their position into adjacent markets, raise barriers to entry and foreclose competition (Konstantopoulou, 2026). In this sense, excessive data leveraging may give rise to non-price exclusionary or leveraging harm, affecting market structure rather than individual users alone (Nayal, 2022).

It has been globally acknowledged by scholars that data practices converge between competition law and data protection law, both protecting distinct outcomes (Abate et al., 2024). On the one hand, data protection regimes seek to protect user rights and regulate the lawful processing of personal information (Protection of Personal Information Act 4 of 2013 s 2). On the other hand, competition law regulates market power and competitive effects (Competition Act 89 of 1998 s 2, as amended). However, the central role in which data plays in digital markets challenges a strictly siloed approach to both regimes (Abate et al., 2024). Adhering to data protection laws may address important rights-based concerns, but it does not necessarily resolve competition issues arising from data concentration or data-driven market power (Costa-Cabral & Lynskey, 2017; O'Callaghan, 2018; Van der Waerdt, 2025). Conversely, competition law intervention does not depend on the existence of a data protection violation, but on the presence of dominance and competitive harm (Abate et al., 2024). This demonstrates that one cannot simply just substitute the one framework for the other.

Therefore, when the interaction between competition law and data protection is acknowledged (May et al., 2023) it should not be construed that their respective mandates should be conflated (There are various approaches proposed to deal with this interaction. See Iacobucci, 2026). Instead, this move reflects the reality that data practices may simultaneously affect the welfare of users and market dynamics (Kshetri, 2014). In the context of abuse of dominance, data protection principles may serve as contextual benchmarks for assessing disproportionality or unfairness (Këllezi, 2019), without displacing competition law's autonomous analysis. This interaction is particularly salient in relation to excessive data collection and data leveraging, which may undermine both consumer welfare and competitive conditions (Choe et al., 2019; Iacobucci, 2026).

The foregoing discussion demonstrates that data practices can generate both exploitative and exclusionary harm in digital markets, even in the absence of monetary pricing (Taufiqurrohman et al., 2025; Abate et al., 2024). Abuse of dominance analysis provides an appropriate lens through which to assess such harm, given its focus on market power, lack of choice, and structural effects. However, whether and to what extent these conceptual considerations are reflected in South African competition jurisprudence remains an open question. In the next section, the legal framework relating to excessive data collection and leveraging is presented.

3. The South African Legal Framework: Abuse of Dominance, Data Protection and Related Aspects

Excessive data collection and leveraging in the digital economy arises largely due to the dominance of the firm in question (Taufiqurrohman et al., 2025). Accordingly, it is important to unpack the legal framework governing dominance and its abuse under South African competition law (Competition Act 89 of 1998 ss 7–9). An abuse of dominance occurs where a firm that holds a dominant position, either by market share or market power, exploits that position by engaging in anti-competitive conduct that harms consumers or forecloses competition (Competition Act 89 of 1998 s 7).

Before turning to the substantive abuse provisions, it is necessary to clarify the scope of application of the Competition Act, as amended. Section 3 of the Competition Act, as amended, provides that it applies to all economic activity occurring within, or having an effect within, South Africa (Competition Act 89 of 1998 s 3, as amended). Importantly, the Competition Act, as amended, does not require that the impugned conduct occur in the same market in which the firm is dominant, nor that the competitive effects manifest in that same market (Nxumalo, 2026). South African jurisprudence has confirmed a broad effects-based approach to jurisdiction and application, and this paper does not revisit that position confirmed by the Courts (*American Natural Soda Ash Corp. & Another v Competition Comm'n of S. Afr.*, 2005, paras. 24–29).

Abuse of dominance is regulated primarily under sections 7, 8 and 9 of the Competition Act (amended). The analytical point of departure is to determine the relevant market (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 33). While abuse of dominance cases typically involve a single relevant market, (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 33) South African competition law recognises that a firm may exercise dominance in one market while the effects of its conduct are felt in another (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 36), and that, in appropriate cases, multiple relevant markets may be implicated (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 33).

Once a determination has been made on defining the relevant market in which the firm operates, the next inquiry is whether the firm in question is dominant (Rudman & Ostrovsky, 2026). Section 7 of the Competition Act (amended) establishes presumptions of dominance based on market share, while also allowing for a finding of dominance below these thresholds where a firm possesses market power (Competition Act 89 of 1998 s 7). Dominance is not determined by market share alone, rather by the ability of a firm to act independently of competitors, customers or consumers. This understanding of dominance is particularly relevant in markets where competitive advantage may derive from control over strategic inputs rather than traditional pricing. It is accepted that control over commercially significant inputs may be used to foreclose rivals and entrench dominance (Competition Act 89 of 1998 ss 8(1)(d)(ii) and (v)), even in the absence of price-based harm.

Once dominance has been established, the second stage of the inquiry requires a determination whether that dominance has been abused (Competition Act 89 of 1998 ss 8–9; Rudman & Ostrovsky, 2026). Prohibited abuses are set out in sections 8 and 9 of the Competition Act (amended) and include a wide range of conduct, such as excessive pricing, refusal to grant access to an essential facility, inducing suppliers or customers not to deal with competitors, refusal to supply scarce goods or services, tying, predatory pricing, margin squeezes, and price discrimination (Competition Act 89 of 1998 ss 8–9). These provisions are framed broadly and are not limited to price-based conduct (Competition Commission).

Exclusionary abuse, by contrast, relates to conduct which excludes or impedes the growth of rivals, thereby entrenching dominance and distorting market structure (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 115). Such conduct is not objectively justified and is liable to be abusive (Padilla, 2026). Exclusionary conduct is harmful because the exclusion of rivals can lead to an increase in the ability of a dominant firm to exercise its market power (Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 115). In Competition Commission and South African Airways, it was observed by the Competition Tribunal that:

“The theory of harm that explains why exclusionary behaviour may be anti-competitive is usually explained in this way. An act that is exclusionary of rivals can lead to the creation of or enhancement of a dominant firm’s ability to exercise market power. By its exercise of market power it can adversely affect consumer welfare by limiting output decisions. As we see this consists of a set of stages of assumptions before we lead to conclusion of welfare loss. Should an abuse of dominance provision that seeks to proscribe exclusionary behaviour require there be evidence of each part of a chain of causation establishing the links from the act of exclusion to the loss of consumer welfare?”

(Competition Comm'n & S. African Airways (Pty) Ltd., 2005, para. 115)

It is important to observe that while the paper focuses on non-price abuses of dominance, in particular those relating to data. However, in practice it is worth noting that abuse of dominance is often tied to vertical restrictive practices. This is dealt with in terms of s 5 of the Competition Act 89 of 1998. Section 5 in a similar way is constituted in two parts – one dealing with the rule of reason in s 5(1) of the Act and the per se

prohibition of minimum resale price maintenance. In terms of s 5(1) of the Competition Act, numerous types of conduct are dealt with such as exclusive dealing, refusal to supply, tying restrictions, exclusive supply, and other vertical arrangements. While these are not per se prohibited, they are dealt with in terms of the substantial lessening of competition effects test (SLC test). In order for there to be a violation of the Competition Act, there must have been an agreement between parties in a vertical agreement such as that between a supplier and a customer or a principal and a distributor which can potentially be justified by a pro-competitive defence.

Visibly, this is very distinct from the process envisaged under sections 8 and 9 of the Competition Act as read with section 7. In principle, the abuse of dominance framework is a unilateral framework in which the dominant firm is the only actor in the matter, as described in the foregoing sections. In contradistinction, the framework pertaining to vertical restraints engages collaborative conduct of parties on different levels of the production chain, with the focus primarily on agreements. This notwithstanding, these two frameworks connect in that the conduct envisaged in these two sections is typically the same. For instance, both sections 5 and 8 engage similar commercial practices such as selective distribution terms, tying agreements or exclusive supply agreements. This entails that, by way of example, if tying restrictions take place and they are not done by a dominant firm, then they would be dealt with under section 5(1) of the Competition Act. At this point, it is worthwhile noting that, historically, there have notably been very few cases that have been adjudicated under s 5(1), meaning that the bulk of cases relating to these issues will be viewed under the abuse of dominance framework. Regardless, s 5 remains the vertical non-price lens. But owing to the fact that most of the vertical restraints undertaken by dominant firms are dealt with in terms of s 8 of the Competition Act, this leaves s 5 of the Competition Act significantly underused.

By way of consideration of the jurisprudence, one can consider cases such as *Competition Commission v Media24* [2019] ZACC 26 which dealt with predatory pricing linked to vertical foreclosure; *Competition Commission v Senwes* [2012] ZACC 6 where the Constitutional Court grappled with a margin squeeze involving a vertically integrated firm and independent downstream firms which were also rivals; or *Computicket v Competition Commission* CAC 170/CAC/Feb19, 2019 which involved exclusive dealing and the blocking of access to rivals. From this brief illustration, it is evident that these are vertical issues which would have been potentially dealt with under s 5(1) had a dominant firm not been involved. It can also be observed from these cases that there is a non-price dimension such as analysis of market access and foreclosure (rather than through price), vertical harm (despite the presence of price harm), and exclusionary vertical foreclosure (despite the application of price-based tests). Thus, while there is a strong representation of price analyses relating to abuse of dominance, it becomes evident that there are also non-price-based considerations that have been made in South African abuse of dominance jurisprudence.

In relation to data protection regulations, excessive data collection implicates several of the core principles governing the lawful processing of personal information under the Protection of Personal Information Act 4 of 2013 (POPIA). In particular, four interrelated principles are engaged: accountability, processing limitation, purpose specification, and further processing limitation (see section 4 of POPIA). The principle of accountability requires the responsible party to ensure compliance with all conditions for the lawful processing of personal information (POPIA, section 8).

Processing limitation, in turn, requires that personal information be processed in a lawful and reasonable manner that does not infringe the rights of data subjects, and that such processing be adequate, relevant, and not excessive in relation to its purpose (POPIA, section 10). Closely related to this is the principle of purpose specification, which requires that personal information be collected for a specific, explicitly defined, and lawful purpose connected to the functions of the responsible party, and that data subjects be informed of that purpose (POPIA, section 13(1)). Further processing of personal information is permitted only to the extent that it is compatible with the original purpose of collection, assessed with reference to factors such as

the nature of the information, the consequences of further processing for the data subject, and the context in which the information was collected.

These principles are directed at protecting individual autonomy, privacy, and informational self-determination, and are inherently non-price in nature. While they play a central role in data protection law, such considerations have not traditionally formed part of the competition law analytical framework, which has focused primarily on price effects, output, and foreclosure. The interaction between these non-price data protection norms and the assessment of abuse of dominance under competition law therefore remains underdeveloped in South African jurisprudence. Having set out the legal regime for abuse of dominance, data protection and related aspects under South African Competition law, in the next section, the implications for abuse of dominance in data-driven markets are considered.

4. Implications for Abuse of Dominance in Data-Driven Markets

In South Africa, the competition jurisprudence has largely focused on price-based and foreclosure-based analyses such as those relating to excessive pricing, resale price maintenance and foreclosure based theories (exclusive dealing, refusal to supply, margin squeezes, and tying and bundling that forecloses rivals), despite the increasing importance of non-price factors such as data practices in digital markets. This pattern reflects the historical development of competition law in markets characterised by monetary exchange and tangible inputs. In contrast, digital markets are frequently structured around zero-price services, non-monetary forms of consideration, and market power derived from the accumulation and strategic use of data (Abate et al., 2024). Scholars have widely observed that traditional competition tools struggle to capture harm in such environments because competition increasingly occurs on dimensions such as quality, privacy, innovation and control over information rather than price alone (Abate et al., 2024). Without recognising this shift, competition enforcement with respect to data-driven harms may prove difficult as the legislative framework remains under-developed in a similar way that interpretation by the courts remains underdeveloped.

This notwithstanding, it is worth noting that the Competition Commission has taken steps to engage with issues pertaining to non-price factors relating to the digital economy by undertaking several market inquiries such as the Online Intermediation Platforms Market Inquiry (OIPMI) and the Media and Digital Platform Markets Inquiry (MDPMI). The findings of the MDPMI are worth consideration. In the MDPMI, the Competition Commission found that access to and use of business data was a competition concern. The Commission also flagged other abuse of dominance related institutions such as self-preferencing, price parity clauses and discriminatory treatment of small and medium enterprises (SMEs) and historically disadvantaged persons (HDPs). With respect to the OIPMI the Commission also considered issues relating to self-preferencing, business-user transaction data access as competition concerns. These inquiries are important because they demonstrate that South African Competition authorities have begun to deal with data access as a non-price competitive parameter. Furthermore, by adopting this approach, the Competition Commission demonstrated that South African authorities were leaning towards an interpretive approach as opposed to a legislative approach in relation to abuse of dominance issues relating to data issues.

This has been supported further by legislative initiatives such as the Competition Amendment Act 18 of 2018 which is partly crafted with the digital/platform dynamics in mind. For instance, the amendments with respect to introduction of provisions relating to avoiding the purchase of goods and services from suppliers that are SMEs or firms that are controlled by HDPs (see section 8(4)(b) of the Competition Act 89 of 1998). Furthermore, another prohibition is included in s 8(1)(d)(iii) of the Competition Act that a seller is prohibited from selling goods or services on the conditions that these goods or products are tied or conditioned to separate goods and services which are unrelated to the object of the contract. This provision was drafted in a technology neutral manner, thus making it adaptable for use to the digital economy, for instance where a seller can tie products together in order to leverage their position in one market to another in an adjacent

market. Moreover, and perhaps more importantly, s 8(1)(d)(iii) is framed as a transformation oriented provision, thus bringing to the abuse of dominance the conversation pertaining to the constitutionalisation of competition law in line with the Preamble of the Competition Act and the purpose provision of the Act. Interestingly, a mirror provision on the seller side is contained in s 9(1A) of the Competition Act which prohibits a dominant firm from avoiding or refusing to sell to SMEs and HDPs in order to avoid price-discrimination rules.

The protection of SMEs and businesses owned by HDPs, to our minds, is a critical issue for the digital environment because this is one area where these categories need further representation and protection. Large businesses, many of which, in our view, have benefited from systematic and structural advantages that linger in South Africa's markets, owing to South Africa's troubled past that is underpinned by a history of racial segregation and separation, has benefited these firms in the past – the benefits of which they have transferred to digital markets. This is necessary if we are serious about achieving a social-justice oriented digital economy (see *Competition Commission of South Africa v Mediclinic Southern Africa (Pty) Ltd and Another* [2021] ZACC 35, para 2).

As observed in *Mediclinic*, it should never be acceptable at any given time that corporate citizens unconscionably focus on any profit margin while disregarding the impact of their conduct on the community, neither should the historic exclusion from meaningful participation for some in the formal economy should not be normalised (*Competition Commission of South Africa v Mediclinic Southern Africa (Pty) Ltd and Another* [2021] ZACC 35, para 3). Notably, the Constitutional Court observed that colonialism, neo-colonialism, and apartheid had institutionalised concentration of ownership and control, building a national economy that is underscored by racial lines, with the corporate sector becoming an exclusive sector for White persons (*Competition Commission of South Africa v Mediclinic Southern Africa (Pty) Ltd and Another* [2021] ZACC 35, para 4). Thus, by advancing an agenda in the digital economy where SMEs and firms owned by HDPs are promoted, progress can be made to free the potential of all persons in the economy in line with the shared commitment in the Constitution of the Republic of South Africa, 1996, that South Africa belongs to all who live in it.

In summary, it can be observed from the conversation above that there have been changes to the legislative framework on abuse of dominance which have to some extent deliberately, and sometimes, inadvertently accommodated non-price considerations in the digital context. It is further noted that, at a practical and enforcement level, the Competition Commission has undertaken the OIPMI and the MDPMI market inquiries, which among other things, engage with non-price issues pertaining to the digital environment. In the section below, we discuss exploitative abuse in zero-price markets.

Exploitative Abuse in Zero-Price Markets

Section 8(1)(a) of the Competition Act (amended) focuses on excessive pricing, assessed through comparisons between price and economic value, thereby emphasising price focused consumer harm. This framework has developed in the context of markets characterised by monetary exchange and does not readily account for the economics of the data-driven economy, where users do not pay with Rands, but with data (Fischer & Miller, 2021).

Where services are provided on a zero-price basis, such benchmarks become difficult or impossible to apply, creating both practical and conceptual obstacles for competition authorities. It becomes inherently difficult to assess whether a “price” is excessive where no monetary price is charged. As a result, conduct involving substantial extraction of value from consumers without monetary payment risks falling outside the scope of traditional excessive pricing analysis. In digital markets, users frequently provide personal data rather than money (Abate et al., 2024), yet South African jurisprudence has not developed tools for evaluating whether

the extent of such extraction is unfair or disproportionate. Furthermore, the lack of development of this legal framework or interpretive framework is problematic in the digital context because, for instance, in certain cases, there is an absence of competitors, or a prior less-data-intensive baseline exists in order to determine what qualifies as excessive pricing.

However, the absence of a monetary price does not imply the absence of exploitation. Value may instead be extracted through non-monetary means, particularly through the collection and use of personal data (Li et al., 2019). Moreover, exploitative abuse is not limited in principle to excessive prices. Abuse of dominance doctrine more broadly recognises that dominant firms may impose unfair trading conditions that extract value disproportionate to what is reasonably required for the provision of a service (Robertson, 2020). This broader conception of unfairness is reflected in the Competition Act itself, which, beyond excessive pricing, recognises unfair trading conditions in contexts such as buyer power abuse, thereby indicating that the statutory framework is not confined to purely monetary conceptions of harm (Competition Act 89 of 1998, s. 8(4)(a)(i)–(ii)) [Although the provision is framed in relation to buyer power abuse, it reflects a broader legislative recognition of unfair trading conditions beyond price-based harm]. The assessment of such conduct may be informed by principles of proportionality, necessity, and justification, focusing on whether the conditions imposed exceed what is required to achieve legitimate commercial objectives. This reasoning does not depend on the existence of a monetary price, but on the relationship between the value demanded and the value provided.

Accordingly, even in the absence of positive pricing, the extraction of extensive personal data as a condition of access to a service may constitute exploitative conduct (Robertson, 2020) where the scope of data demanded is disproportionate to the service offered or to user's reasonable expectations. The challenge posed by zero-price markets is therefore methodological rather than conceptual. The Competition Act's prohibition of abuse of dominance is sufficiently broad to encompass non-monetary exploitation, provided that analytical tools are adapted to account for data as a form of consideration.

Exclusionary abuse and data-driven market power

Unlike exploitative abuse, exclusionary abuse doctrine is not anchored in price, but in the assessment of foreclosure and its effects on the competitive process. This renders it, in principle, more adaptable to digital markets, where market power is often exercised through control over strategic inputs rather than through pricing conduct. South African jurisprudence has recognised that dominance may be entrenched through control over inputs that are necessary for rivals to compete effectively, particularly where such control raises barriers to entry or expansion.

In digital markets, consumer data may perform a comparable function. The accumulation and control of large volumes of user data can confer significant competitive advantages, enabling firms to improve product quality, refine targeting, and reinforce network effects. Access to such data may therefore constitute a critical input for effective competition, particularly where rivals are unable to replicate the scale, scope, or historical depth of incumbent datasets.

Notwithstanding this conceptual flexibility, South African abuse of dominance jurisprudence has not yet treated data as a strategic input capable of generating exclusionary effects. Practices such as data aggregation across services, preferential access to user information, or the leveraging of data across markets have not been systematically analysed as mechanisms of foreclosure. This omission is partly attributable to the absence of a clear analytical distinction between data collection and data use, which limits the ability of competition authorities to identify how data advantages are translated into market power.

The limitation is therefore not doctrinal, but analytical. Section 8(1)(c) of the Competition Act is sufficiently broad to encompass exclusionary conduct arising from control over data, provided that data is recognised as a competitive input capable of foreclosing rivals. The challenge lies in adapting existing analytical tools to reflect how market power is exercised in data-driven markets.

5. Comparative Insights on Data, Privacy And Competition: Case Law on Exploitative Abuses

While the findings of foreign courts are not binding in South Africa, foreign cases have persuasive value and offer instructive lessons for future regulation (Constitution of the Republic of South Africa, 1996, s. 39(1)(c); Rautenbach, 2020). Four cases have been selected as comparative case studies. These are discussed below.

5.1 Karmanya Singh Sareen v. Union of India & Others, W.P. (C) 7663 of 2016

This case, which was initiated in 2016, was based on claims by users of WhatsApp that WhatsApp's privacy policy infringes the privacy policy of users because it allowed WhatsApp to share data with Facebook and all its group of companies for the purposes of commercial advertising and marketing (Karmanya Singh Sareen v Union of India, para. 2). The High Court decision illustrates that dominant digital platforms may leverage their market position to collect user data in ways that undermine privacy (Karmanya Singh Sareen v Union of India, para. 17).

Accordingly, the High Court, having considered that consumers have an option to opt out of WhatsApp (the so-called take it or leave it option), provided that WhatsApp users who decided to delete their accounts by 25.09.2016 would have their data completely deleted from WhatsApp and not subsequently shared with Facebook or any of its group of companies (Karmanya Singh Sareen v Union of India, para. 20). In the case of consumers who opted to remain on WhatsApp, their data up to 25.09.2016 would not be shared with Facebook or any of its group of companies (Karmanya Singh Sareen v Union of India, para. 20). Finally, it was stated that the Union of India and the Telecom Regulatory Authority of India has to take measures to ensure that the functioning of the Internet Messaging Applications “like ‘WhatsApp’ and take an appropriate decision at the earliest as to whether it is feasible to bring the same under the statutory regulatory framework” (Karmanya Singh Sareen v Union of India, para. 20).

In ruling in favour of WhatsApp, the court stated that:

“In fact, the users of “WhatsApp” and [WhatsApp] are parties to a private contract, and the users of “WhatsApp” having voluntarily opted to avail services of the said Application, are bound by the terms of service offered by [WhatsApp]. [...] Under the privacy policy of “WhatsApp”, the users are given an option to delete their “WhatsApp” account at any time, in which event, the information of the users would be deleted from the servers of “WhatsApp”. We are therefore of the view that it is always open to the existing users of “WhatsApp” who do not want their information to be shared with Facebook to opt for deletion of their account”

(Karmanya Singh Sareen v Union of India, para. 19). (emphasis added)

So, therefore, the leveraging of data with Facebook and group of companies was allowed after 25.09.2016 (Karmanya Singh Sareen v Union of India, para. 20). The Delhi High Court upheld the 2016 WhatsApp policy update and dismissed the petition application (WhatsApp LLC v Competition Commission and Others, 2025, para. 8).



Soon after, the petitioners filed an appeal with the Supreme Court (*Karmanya Sareen v Union of India*, 2017). The Supreme Court hearing dealt with 3 main issues, specifically: (1) whether WhatsApp's 2016 privacy policy violated users' rights to privacy, (2) whether a privacy policy should have 'specific 'opt-out' provisions without the user having to opt out of the app in totality (in other words, whether there should be an opt out button for WhatsApp to share data with Facebook and its group of companies), and (3) whether the manner of seeking consent from users who are unable to understand the terms and conditions of the new privacy policy deception. The Supreme Court held that existing users always had an option to delete their accounts if they did not want to share that information. The constitutional bench of the Supreme Court further opposed the granting of interim relief (*WhatsApp LLC v Competition Commission and Others*, 2025, para. 10). It was contended in the matter that:

"(i) the 2021 Update vitiates informed consent; and (ii) the 2021 Update violates fundamental privacy principles (IFF Application). An application filed by the Petitioner in Karmanya, Hon'ble Supreme Court seeking similar reliefs against the 2021 Update was disposed of by the Hon'ble Supreme Court on 1 February 2023 without granting any injunctive relief against the 2021 Update"

(*WhatsApp LLC v Competition Commission and Others*, 2025, para. 9).

The above notwithstanding, to our minds, what also emerged from this case, although not raised in this case, was the need for regulatory frameworks that address both competition and data protection concerns as well as the regulatory collaboration that is needed in these instances. It was a missed opportunity for the courts in India to discuss the issue of market power and dominance. It would have been interesting for the matter to consider the prevailing network effects and the switching costs of users before coming to a decision that consumers had an option to delete their accounts. Further to this, it had to also be observed that WhatsApp and its parent company, Facebook, are a big organisation whose services cannot be easily replicated. Therefore, while consumers had the option to delete their accounts, there was no easy substitute for this product (considering metrics such as user numbers, integration, among others).

Accordingly, it can thus be said that WhatsApp was able to leverage its market power to impose such terms on consumers. This matter thus involved a non-price parameter that impacted competition in relation to a multi-side platform. To this end, Shah and Tomar argue that the Delhi High Court did not consider that leveraging of data across platforms as a precondition to using WhatsApp services amounts to imposition of unfair conditions, which stems from WhatsApp's dominance in the market of communication services (Shah & Tomar, 2022). In other words, there was an opportunity to consider whether the collection of data by WhatsApp and the potential to have anti-competitive effects, in particular, exploitative and exclusionary effects (Shah & Tomar, 2022). It must however be noted that since the 2016 and 2017 cases, there have been a number of developments. For instance, in 2019 the government of India introduced the Personal Data Protection Bill, 2019 which was subsequently withdrawn in 2021 and replaced by the Digital Personal Data Protection Act, 2023, which is the current regulatory position with respect to the protection of data. With respect to the *Karmanya Singh v Union of India* case, similar proceedings were launched in the courts in 2021. Nonetheless, in 2021, the *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users Suo Moto*, 2021 (Case No. 1 of 2021) was instituted in which competition and data protection issues were considered in relation to WhatsApp's usage policy updates. Before we turn to the discussion on *Suo Moto*, we will first consider the case of *Shri Vinod Kumar Gupta, Chartered vs Whatsapp Inc.* (Case No. 99 of 2016.).

5.2 *Shri Vinod Kumar Gupta, Chartered vs Whatsapp Inc, 2016*

This was an order of the Competition Commission of India which was filed by Shri Vinod Kumar Gupta (Informant) under Section 19(1)(a) of the Competition Act, 2002 against WhatsApp Inc for an alleged violation of s 4 of the Competition Act (Shri Vinod, para. 1). The Informant submitted that the relevant product market

was the ‘free messaging’ market for various smartphones (Shri Vinod, para. 4). The relevant geographic market would be the global market (Shri Vinod, para. 4). In the smartphone market with about 95% of Android devices, amounting to about 70 million users, having WhatsApp. (Shri Vinod, para. 4) Thus, WhatsApp held a substantial market in India (Shri Vinod, para. 4) . At a global level, WhatsApp had clear market domination in 109 countries, thus controlling a 55.5% world market share.

Initially, WhatsApp had started with a one-year free trial which was followed by a fee of USD 0.99 levied yearly (Shri Vinod, para. 5). However, it is contested that, by January 2016, WhatsApp had stopped charging this fee leading to it foregoing its only source of revenue, turning it into a free service (Shri Vinod, para. 5). Resultantly, its customer base, globally, rose from USD 450 million to USD 1 billion (Shri Vinod, para. 5). It was alleged that WhatsApp was able to provide services freely by sourcing funds from its parent company, Facebook (Shri Vinod, para. 5). In the view of the informant, this constituted predatory pricing in violation of the Competition Act (Shri Vinod, para. 5). It was further alleged that, by mandating users to agree with its privacy terms and conditions in August 2016, WhatsApp has been leveraging this data with Facebook for targeted advertisements (Shri Vinod, para. 6). It is averred that the manner through which the consent is obtained for this process by WhatsApp is deceptive (Shri Vinod, para. 6). The rationale behind this argumentation is that users in India are not suitably equipped to read and understand the terms and conditions, including those relating to privacy (Shri Vinod, para. 6). To this end, it was argued that the respondent was in violation of s 4 of the Competition Act (Shri Vinod, para. 6).

Further to this, and from an information communication perspective, the new privacy policy would allow WhatsApp to copy/extract/download information from the mobile phone’s database, inclusive of critical information such as contacts in violation of the Information Technology Act 2000 (Shri Vinod, para. 6). It was therefore the prayer of the informant that the Commission investigate the alleged anticompetitive conduct which was abusive in nature (Shri Vinod, para. 7). It sought an order that prohibited WhatsApp from leveraging data with Facebook and directing WhatsApp to not disconnect services to those that did not ‘opt in’ into the new privacy rules (Shri Vinod, para. 7).

In considering whether there was a violation of competition rules pertaining to the abuse of dominance would first require a determination of the relevant product market or relevant geographical market (Shri Vinod, para. 10-11). Effectively, in this case, the relevant product market that was thus ‘the market for instant messaging services using consumer communication apps through smartphones’ (Shri Vinod, para. 11). In terms of the relevant geographic market, this was considered to be India, despite the functionality of the application as being cross-border (Shri Vinod, para. 12). In other words, the relevant market is “the market for instant messaging services using consumer communication apps through smartphones in India” (Shri Vinod, para. 13). With respect to dominance, the Commission found WhatsApp to have a 56% share of internet users in India and Facebook as having a 51% user base (Shri Vinod, para. 14).

On the issue of abuse of dominance, the Commission observed that WhatsApp was abusing its dominant position in the relevant market by introducing privacy policy requirements which compel users to share their account details and information with Facebook (Shri Vinod, para. 15). The policies were geared at improving Facebook’s advertising and product experiences (Shri Vinod, para. 15). WhatsApp however contended that Facebook and its family of companies would utilise the information to improve infrastructure and delivery systems, fighting spam, abuse or infringement activities (Shri Vinod, para. 15). It had been averred, by the informant, that this leveraging of data should be prohibited because it violates the privacy and safety of users in contravention of the Information Technology Act 2000 (Shri Vinod, para. 16). This was further compounded by allegations of predatory pricing owing to WhatsApp not charging a user fee. (Shri Vinod, para. 18).

It is also important to note that the Commission was of the view that there were no major switching costs owing to the fact that: (Shri Vinod, para. 18) (a) all consumer communication apps are offered for free of cost

or at a very low price (mostly free), (b) all consumer communication apps are easily downloadable on smartphones and can co-exist on the same handset (also called 'multi homing') without taking much capacity along with other apps, and (c) once consumer communication apps are installed, (d) consumer communication apps are normally characterised by simple user interfaces so that costs of switching to a new app are minimal for consumers, and (e) information about new apps is easily accessible given the ever increasing number of reviews of consumer communication apps on app stores like Google Play Store etc.

Against the backdrop of the above analysis, the Commission found that while WhatsApp appeared to be dominant in the relevant market, the allegations of predatory pricing therefore, in its view, had no merits (Shri Vinod, para. 19). Accordingly, the Commission found that there was no contravention of the Competition Act (Shri Vinod, para. 19). The National Company Law Appellate Tribunal (NCLAT) in August 2022, on appeal, in the Vinod Kumar Gupta v. Competition Commission of India, Competition Appeal No. (AT) 13 of 2017 (Vinod Gupta NCLAT) upheld the decision of the Commission to dismiss the allegations of abuse of dominance on the basis of the 2016 update (WhatsApp v Competition Commission, para. 11).

5.3 In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users Suo Moto, 2021

In Suo Moto, which was an order of the Competition Commission of India, it was evaluated whether the policy updates could be examined in terms of s 4 of the Competition Act, 2002 (Suo Moto Case No. 1 of 2021, para. 14). Section 4 of the Indian Competition Act provides a prohibition against the abuse of dominance. It provides that there shall be no abuse of dominance, directly or indirectly, which imposes unfair or discriminatory on the condition in the purchase or sale of a good or service or price in purchase or sale (including predatory price) of goods or service (Indian Competition Act, 2002, s. 4). Furthermore, s 4 limits the abuse of a dominant position which limit or restrict the production of goods and services or market; or technical or scientific developments relating to goods or services; or indulges in practice or practices resulting in denial of market access; or makes conclusion of contracts subject to acceptance by other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts; or uses its dominant position in one relevant market to enter into, or protect, other relevant market (Indian Competition Act, 2002, s. 4).

The Commission observed in this matter that under competitive market conditions, would have the sovereign rights and control over decisions pertaining to their personal data (Suo Moto Case No. 1 of 2021, para. 28). However, it was noted that this was not the case with WhatsApp and there appeared to be no plausible reason as to why users had no control or say over such cross-product processing of their data by means of voluntary consent as opposed to it being a pre-condition for availing WhatsApp's service (Suo Moto Case No. 1 of 2021, para. 28). It was further noted that, previously, consumers had been given control with respect to the sharing of their personal data with Facebook, particularly with respect to the 'opt out' provision that was available for 30 days in previous policy updates (Suo Moto Case No. 1 of 2021, para. 29). This time around however, this has not been done (Suo Moto Case No. 1 of 2021, para. 29). To this end, the Commission observed that:

"Thus, users are required to accept the unilaterally dictated 'take-it-or-leave-it' terms by a dominant messaging platform in their entirety, including the data sharing provisions therein, if they wish to avail their service. Such "consent" cannot signify voluntary agreement to all the specific processing or use of personalised data, as provided in the present policy. Users have not been provided with appropriate granular choice, neither upfront nor in the fine prints, to object to or opt-out of specific data sharing terms, which prima facie appear to be unfair and unreasonable for the WhatsApp users"

(Suo Moto Case No. 1 of 2021, para. 29).

Following a careful consideration of the facts around the matter, the Commission was of the view that the sharing of consumers' user data with Facebook and its other entities by WhatsApp in a manner that was not transparent and lacking user consent (voluntary and specific), appeared to be unfair on the face value to users (Suo Moto Case No. 1 of 2021, para. 30). It was noted that the purpose of the sharing of the data seemed to be unaligned with consumers' reasonable and legitimate expectations with respect to quality, security or any other relevant aspects for which they registered on WhatsApp (Suo Moto Case No. 1 of 2021, para. 30). For instance, one of the reasons furnished for the sharing of the data pertained to the need to build consumer user profiles through cross-linking of data collected across services (Suo Moto Case No. 1 of 2021, para. 30). Rightfully, the Commission highlighted that 'such data concentration' had the ability to raise competition concerns in instances in which it could be said to create competition concerns (Suo Moto Case No. 1 of 2021, para. 30). Accordingly, the Commission observed that:

"The impugned conduct of data-sharing by WhatsApp with Facebook apparently amounts to degradation of non-price parameters of competition viz. quality which result in objective detriment to consumers, without any acceptable justification. Such conduct prima facie amounts to imposition of unfair terms and conditions upon the users of WhatsApp messaging app, in violation of the provisions of Section 4(2)(a)(i) of the Act"

(Suo Moto Case No. 1 of 2021, para. 30).

In the view of the court, WhatsApp owing to the enhanced network effects it enjoys and the lack of any noteworthy competitor within the instant messaging market in India could compromise quality in relation to the protection of individualised data (Suo Moto Case No. 1 of 2021, para. 31). In addition, WhatsApp had the capacity to impose friendly terms such as 'opt-out' choices without risking the loss of its database but chose not to (Suo Moto Case No. 1 of 2021, para. 31). Furthermore, users of WhatsApp who did not want to continue with WhatsApp would have a grave challenge of potentially losing their historic data (Suo Moto Case No. 1 of 2021, para. 31). This was because the process of porting to competing apps was extremely cumbersome and time consuming (Suo Moto Case No. 1 of 2021, para. 31). Notably, network effects would also potentially make this process of switching apps difficult (Suo Moto Case No. 1 of 2021, para. 31). As a result, consumers that were affected by the policy changes would face enhanced switching costs (Suo Moto Case No. 1 of 2021, para. 31). The Commission went on to state that:

"Today's consumers value non-price parameters of services viz. quality, customer service, innovation, etc. as equally if not more important as price. The competitors in the market also compete on the basis of such non-price parameters. Reduction in consumer data protection and loss of control over their personalised data by the users can be taken as reduction in quality under the antitrust law. Lower data protection by a dominant firm can lead to not only exploitation of consumers but can also have exclusionary effects as WhatsApp/Facebook would be able to further entrench/reinforce their position and leverage themselves in neighbouring or even in unrelated markets such as display advertising market, resulting in insurmountable entry barriers for new entrants"

(Suo Moto Case No. 1 of 2021, para. 32).

In the view of the Commission, data and data analytics had great importance for the competitive performance of digital enterprises (Suo Moto Case No. 1 of 2021, para. 33). Accordingly, the cross-linking and integration of user data could further strengthen data advantages in addition to safeguarding and reinforcing the market power of dominant firms (Suo Moto Case No. 1 of 2021, para. 33). It was further said that:

"For Facebook, the processing of data collected from WhatsApp can be a means to supplement the consumer profiling that it does through direct data collection on its platform, by allowing it to track users and their communication behaviour across a vast number of locations and devices outside Facebook platform."

Therefore, the impugned data sharing provision may have exclusionary effects also in the display advertising market which has the potential to undermine the competitive process and creates further barriers to market entry besides leveraging, in violation of the provisions of Section 4(2)(c) and (e) of the Act”

(Suo Moto Case No. 1 of 2021, para. 33).

The Commission observed that it was possible, as per the 2021 update to the privacy policy, that a business could provide a third-party service provider such as Facebook with access to its information (Suo Moto Case No. 1 of 2021, para. 33). This involved such providing sending, storing, reading, managing or otherwise process them for the business (Suo Moto Case No. 1 of 2021, para. 33). It was therefore plausible that Facebook could condition this process to the use of such data collected (Suo Moto Case No. 1 of 2021, para. 33). In the view of the court, all these matters had to be investigated by the Director General. Based on these considerations, the Commission was of the view that WhatsApp had prima facie violated s 4 of the Competition Act through its exploitative and exclusionary conduct as was observed in this matter (Suo Moto Case No. 1 of 2021, para. 34). It noted that a full and detailed investigation was required in order to determine “the full extent, scope and impact of data sharing through involuntary consent of users” (Suo Moto Case No. 1 of 2021, para. 34). To this end, the Commission directed the Director General (DG) to cause an investigation under s 21 of the Indian Competition Act and submit a report within 60 days of the receipt of this order (Suo Moto Case No. 1 of 2021, para. 35). WhatsApp and Facebook had the opportunity to make oral submissions in response in a hearing before the Commission (Suo Moto Case No. 1 of 2021, para. 35). Importantly, it was noted that nothing in the order would amount to a final expression of the merits of the matter and that the DG still had to conduct an investigation without being swayed by the observations contained in the order (Suo Moto Case No. 1 of 2021, para. 38).

Pursuant to the order above, the DG submitted an Investigation Report (confidential and non-confidential versions) on the 12th of January 2023 (WhatsApp v Competition Commission, para. 17). Following this report, the Commission issued an order on the 18th of November 2024 (WhatsApp v Competition Commission, para. 17). The Commission found that the relevant markets were the OTT messaging apps through smartphones in India and the market for online display advertising in India (WhatsApp v Competition Commission, para. 17). The Commission found that Meta was dominant in the first market with respect to OTT messaging apps market (WhatsApp v Competition Commission, para. 17). Further to this, the Commission found that Meta, through WhatsApp, had abused its dominance in contravention of s 4 of the Competition Act (WhatsApp v Competition Commission, para. 17). More specifically, it was observed that Meta, through WhatsApp, had abused its dominance by (WhatsApp v Competition Commission, para. 17):

- a) coercing WhatsApp users to accept allegedly expanded user data collection and sharing with the “Meta group” without an opt-out under the 2021 Update (violating Section 4(2)(a)(i) of the Competition Act, 2002 (Competition Act));
- b) sharing WhatsApp user data with Meta companies for purposes other than providing the WhatsApp service, resulting in the denial of access to the alleged market for “online display advertisements in India” (violating Section 4(2)(c) of the Competition Act); and
- c) leveraging its alleged dominance in the alleged market for “OTT messaging apps through smartphones in India” to protect its position in the online display advertising market (violating Section 4(2)(e) of the Competition Act).

Owing to these findings, a penalty of ₹213.14 crore (approximately USD 25.25 million) and a 5-year restriction on sharing WhatsApp user data with other Meta Companies was imposed (WhatsApp v Competition Commission, para. 4). Meta was also, in terms of s 27(a) of the Competition Act, directed to cease and desist from indulging in anti-competitive practices that have been found to be in violation of s 4 of the Competition

Act, as detailed in the order (WhatsApp v Competition Commission, para. 7). For data that was shared for purposes other than advertising, Meta had to include in WhatsApp's policy an explanation of the data that was shared with Meta and the purpose of the data sharing (WhatsApp v Competition Commission, para. 17). The data to be shared and the purpose of the sharing of data had to be specified (WhatsApp v Competition Commission, para. 17).

In addition to this, where data was shared for purposes other than providing WhatsApp services, all users in India had to have had the option to manage such data sharing by means of an opt-out option mainly by way of an in-app notification (WhatsApp v Competition Commission, para. 17). Further to this, all users in India would also be furnished with an option to review and modify their choice with respect to the sharing of such data via a prominent tab in the WhatsApp settings tab (WhatsApp v Competition Commission, para. 17). Importantly, it had to be noted that all future updates had to comply with these requirements (WhatsApp v Competition Commission, para. 17). WhatsApp and Facebook were then directed to comply with these directions within 3 months from the date of the order (WhatsApp v Competition Commission, para. 17). Also, these parties had to furnish the Commission with a compliance report (WhatsApp v Competition Commission, para. 17).

5.4 *WhatsApp LLC v Competition Commission and Others, 2025*

This judgement which was passed in 2025 concerned two appeals against an order that had been passed by the Competition Commission in November 2024 (WhatsApp v Competition Commission, 2025, para. 1). In this order, the Competition Commission of India had found that Meta had abused its dominance through the imposition of a 2021 privacy policy which imposed unfair conditions on users by leveraging its dominance in the Over-the-Top (OTT) messaging application market (WhatsApp v Competition Commission, 2025, para. 2). Subsequently, the Commission imposed a ₹213.14 crore penalty (approximately USD 25.25 million) and a 5-year restriction on sharing WhatsApp user data with other Meta Companies (WhatsApp v Competition Commission, 2025, para. 2).

In deliberating this matter, the Commission also discussed privacy as a competition concern and the interplay of competition law with data-protection law, and the exclusivity or complementarity jurisdiction of the Competition Commission of India (WhatsApp v Competition Commission, 2025, para. 31). It was argued by the appellants that the Commission went beyond its jurisdiction and made findings on privacy and data protection issues (WhatsApp v Competition Commission, 2025, para. 31). In the view of the appellants, these issues fall outside the realm of matters canvassed by competition authorities (WhatsApp v Competition Commission, 2025, para. 31). To their mind, these issues would be covered by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) or the Digital Personal Data Protection Act, 2023 (DPDP Act) or draft DPDP Rules (WhatsApp v Competition Commission, 2025, para. 31).

The parties asserted that the challenged order of the Commission was based on "the adequacy of user consent, transparency of privacy disclosures, and purpose limitation in the processing of personal data"- all of which are dealt with by the aforementioned data rules (WhatsApp v Competition Commission, 2025, para. 31). In the view of these parties, the mandate of the Commission pursuant to the Competition Act was that its operations were limited to examining instances where there was an appreciable adverse effect on competition in a relevant market (WhatsApp v Competition Commission, 2025, para. 31). This, to their belief, did not extend to the determination of compliance with privacy or data protection standards (WhatsApp v Competition Commission, 2025, para. 31). These parties observed that, the moment the Competition Commission realised that it was required to deliberate on the matter of sufficiency of consent or the lawfulness of processing data, it should have then exercised restraint and then subsequently deferred the exercise of this decision to the relevant authorities (WhatsApp v Competition Commission, 2025, para. 31).



To this end, the thinking of these parties was therefore that the Commission had descended into an area that way beyond its statutory expertise (WhatsApp v Competition Commission, 2025, para. 31). Accordingly, the weighted consideration of these parties was that the findings of the Commission were ultra vires and therefore had to be set aside (WhatsApp v Competition Commission, 2025, para. 31). In support of this view, the appellants demonstrated the importance of data protection legislation and how the right to privacy which is protected by such legislation had evolved (WhatsApp v Competition Commission, 2025, para. 32). The parties cited the matter of K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC which established the right to privacy as a fundamental right that is protected under Article 21 of the Indian Constitution (WhatsApp v Competition Commission, 2025, para. 32).

The court, in this case, considered privacy as a fundamental right or liberty pursuant to Article 21 of the Indian Constitution (WhatsApp v Competition Commission, 2025, para. 32). This provision reads: No person shall be deprived of his life or personal liberty except according to procedure established by law” (WhatsApp v Competition Commission, 2025, para. 32). In view of the court, privacy involved “personal autonomy, bodily integrity, the right to self-determination, and informational privacy”, values of which are critical and relevant to the digital economy (WhatsApp v Competition Commission, 2025, para. 32). The judgment underscored that the right to privacy was not absolute and it could be restricted in instances where state action was lawful, legitimate, proportionate and necessary (WhatsApp v Competition Commission, 2025, para. 32).

The appellants noted that they had been made aware that the Puttaswamy judgement had resulted in the establishment of the DPDP Act – thus establishing the basis upon which privacy protections in Indian law are operationalised (WhatsApp v Competition Commission, 2025, para. 32). The DPDP Act had its foundation upon principles covered in the Puttaswamy judgement such as informed consent, purpose limitation, and data minimisation (WhatsApp v Competition Commission, 2025, para. 32). The Act also “establishes rights for individuals (data principals) like access, correction, and erasure of personal data, seeking to uphold individual autonomy against state and private interference” (WhatsApp v Competition Commission, 2025, para. 32). The DPDP Act attempts to balance privacy interests with legitimate interests of the state such as national security (WhatsApp v Competition Commission, 2025, para. 32). The parties observed that, the Act, which was inspired by Puttaswamy, considered matters such as collection, the processing of personal data, consent and autonomy, amongst others (WhatsApp v Competition Commission, 2025, para. 32).

This notwithstanding, the NCLAT noted that competition law, as enforced by the Competition Commission India, has had to now deal with new kinds of matters such as unfair data practices wherein users are required to consent to data collection as a condition of service, which has been separately taken up by the Commission (WhatsApp v Competition Commission, 2025, para. 32). The appellants contested this, noting that for the Competition Commission to be able to make a violation, it would first have to make findings on privacy and data protection issues - for which it lacks jurisdiction (WhatsApp v Competition Commission, 2025, para. 32).

Against this backdrop, the appellants held the view that the judgment dated 18 November 2024, which is contended in this matter, was underpinned by those findings (WhatsApp v Competition Commission, 2025, para. 32). The Commission should, as done in previous matters such as Vinod Kumar Gupta v. Competition Commission of India, Competition Appeal No. (AT) 13 of 2017 and Winzo Games Private Limited v. Google LLC and Others, Case No. 42 of 2022 (WhatsApp v Competition Commission, 2025, para. 32). In actual effect, the appellant took the view that only after these matters had been dealt with by the data protection authorities, only would the Commission then step in to deal with competition issues, from a competition perspective (WhatsApp v Competition Commission, 2025, para. 32).

The Commission however strongly rejected the above arguments by Meta and Facebook (WhatsApp v Competition Commission, 2025, para. 32). In its view, there was no conflict between the Competition Act and

the authority of the data protection regulators pursuant to data protection and privacy laws (WhatsApp v Competition Commission, 2025, para. 32). In this regard:

“The CCI explains that it is not examining whether WhatsApp’s policy violates privacy statutes but whether WhatsApp’s conduct of requiring users to share data with Meta amounts to an abuse of dominance under Section 4 of the Competition Act. It maintains that privacy and data collection practices can influence competition because they affect consumer choice, quality, and fairness in the market. Therefore, the CCI’s focus is on the competitive impact of WhatsApp’s data-sharing arrangements, while compliance with data protection obligations remains within the domain of sectoral regulators, making the two frameworks complementary rather than conflicting”

(WhatsApp v Competition Commission, 2025, para. 36).

The Commission therefore was of the view that the appellants had a narrow view of competition law (WhatsApp v Competition Commission, 2025, para. 37). Data protection and privacy laws deal with a narrower category of data, specifically, sensitive personal data and identifiable user information (WhatsApp v Competition Commission, 2025, para. 37). In contradistinction, competition law concerns non-personal data, non-sensitive data and significantly broader categories of data which are utilised by dominant entities (WhatsApp v Competition Commission, 2025, para. 37). The Commission also noted that reliance by the appellant on competition matters such as Shri Vinod Kumar Gupta vs. CCI & Ors. CA(AT) No. 13 of 2017 which upheld the 2016 WhatsApp policy updates (WhatsApp v Competition Commission, 2025, para. 38).

In the view of the Commission, this was because there was a notable difference between the 2016 and 2021 policies, with the 2021 policy being significantly expansive in the manner that data was collected and shared (WhatsApp v Competition Commission, 2025, para. 38). Furthermore, it was noted that the order of the Commission was based on s 26(2) of the Indian Competition Act that allows matters to be closed at the initial stage without ordering an investigation (WhatsApp v Competition Commission, 2025, para. 38). Rather, the matter was dealt with utilising the content of the information received by the Commission (WhatsApp v Competition Commission, 2025, para. 38). Owing to the fact that this was an in limine dismissal, the Commission lacked the benefit of a detailed investigation by the DG (WhatsApp v Competition Commission, 2025, para. 38). Contrary to this approach, the order challenged is one that was given in terms of s 27 of the Indian Competition Act following a detailed investigation whereupon cogent evidence is adduced (WhatsApp v Competition Commission, 2025, para. 38).

Moreover, it was argued by the Commission that the order relied upon by the appellants was a 2017 one (WhatsApp v Competition Commission, 2025, para. 40). Since then however, much has changed owing to the fast-changing pace of the digital environment (WhatsApp v Competition Commission, 2025, para. 40). Furthermore, it is also important to note that the decisions relied upon were decisions of the Commission which is bound by decisions of the Tribunal (NCLAT), which imposed the 2024 order (WhatsApp v Competition Commission, 2025, para. 41). The Commission can only depart from these findings in the event that it had cogent evidence demonstrating that there had been a significant change in 2021 update from the 2016 update, changes and evidence of which are unavailable in the present matter (WhatsApp v Competition Commission, 2025, para. 41). Another important point was in relation to the fact that a DG investigation was not ordered in relation to the 2016 update owing to the fact that there was an opt-out provision provided by WhatsApp, which has not been afforded to consumers in this case through the 2021 update (WhatsApp v Competition Commission, 2025, para. 42).

In engaging the relevant rules with the facts of the matter, the Tribunal made the following finding:



“We find that even though the DPDP Act 2023, governs the collection and processing of personal data, prioritizing consent and autonomy, however, Competition law, enforced by the Competition Commission of India (CCI), prevents abuse of dominance and anti-competitive practices, which we have found in this case to include unfair data practices such as forcing users to consent to data collection as a condition for service”

(WhatsApp v Competition Commission, 2025, para. 44).

The Tribunal also found that the reliance of the appellants on Vinod Kumar Gupta v. Competition Commission of India, Competition Appeal No. (AT) 13 of 2017 (Vinod Kumar Gupta) was misguided on the basis that the 2016 and 2021 policies were fundamentally different (WhatsApp v Competition Commission, 2025, para. 45). In addition to this, the order of the Commission was preliminary in terms of s 26(2) of the Indian Competition Act, while the contested order was a final order in terms of s 27 of the Competition Act (WhatsApp v Competition Commission, 2025, para. 45). Similarly, it was noted that the case of Winzo Games Private Limited v. Google LLC and Others, Case No. 42 of 2022 (Winzo) which was relied upon by the appellants was deemed inappropriate as the factual matrix was vastly different to the present circumstances (WhatsApp v Competition Commission, 2025, para. 46). The NCLAT observed that the DPDP Act and the related draft rules could not oust the jurisdiction of the competition authorities (WhatsApp v Competition Commission, 2025, para. 47). It went on to note that:

“Finally, we find that the CCI’s function is distinct from that of sectoral or privacy regulators: it evaluates competitive effects of conduct, such as forced data-sharing, regardless of whether data protection statutes are also engaged. Thus, the arguments reinforce that CCI retains both the mandate and necessity to address privacy-related competitive harms. We also note that Privacy is recognized by competition regulators worldwide as a critical non-price competition parameter, valued by users on par with quality, customer service, and innovation and this is also elaborated by us separately. Per above analysis we don’t find any conflict between CCI’s jurisdiction under the Competition Act and the authority of data protection regulators under the IT Act or privacy laws”

(WhatsApp v Competition Commission, 2025, para. 50 - 52).

The above analysis is critical in demonstrating that the competition authorities are not interfering with the mandate of data protection authorities but are simply enforcing competition rules in a data protection related scenario. The Tribunal went on to say that:

“We also find that CCI is not examining whether WhatsApp’s policy violates privacy statutes but whether WhatsApp’s conduct of requiring users to share data with Meta amounts to an abuse of dominance under Section 4 of the Competition Act. We agree with the arguments of the CCI that privacy and data collection practices can influence competition because they affect consumer choice, quality, and fairness in the market. We also find that CCI has focussed on the competitive impact of WhatsApp’s data-sharing arrangements/ data leveraging, while compliance with data protection obligations remains within the domain of sectoral regulators, making the two frameworks complementary rather than conflicting”

(WhatsApp v Competition Commission, 2025, para. 52).

It was further explained by the Tribunal that:

“We can thus conclude that the Commission’s jurisdiction encompasses not just overtly anti-competitive economic practices but also extends to unfair data practices that may affect competition dynamics, consumer choice, and market fairness. The DPDP Act’s existence does not make the CCI redundant; rather, both frameworks operate complementarily, where competition regulation addresses practices influencing market

power, irrespective of overlap with privacy laws. Moreover, each new policy or conduct (such as the much broader 2021 WhatsApp policy) can merit fresh investigation notwithstanding prior decisions or regulatory action, as markets and business conduct evolve rapidly”

(WhatsApp v Competition Commission, 2025, para. 53).

The Tribunal as observed above, did well in highlighting the synergies between the competition law framework and the data protection and privacy frameworks. It brings to the fore the understanding that the existence of data protection rules does not undercut the mandate of the Commission to deal with anticompetitive practices such as unfair data practices. The Tribunal also referred to the issue of zero-price market economics, noting that:

“We note the pivotal role played by data in the operation of digital platforms. Business Entities are able to provide zero-priced products only because there is value attached to the vast amount of data that is collected from their users. We note that this Tribunal’s judgment in Google LLC & Anr. vs. Competition Commission of India CA (AT) No. 10 of 2023 (Paras 210 to 213) has set out the central role played by data in zero-priced multi-sided digital markets (while specifically referring to advertising) and competition concerns arising therefrom. In digital markets, an enterprise’s competitive advantage is increasingly shaped by the amount, diversity, and quality of data it possesses access to such data has become a crucial source of market power, as it allows platforms to improve services, target users more effectively, and operate more efficiently than their competitors (as recognised in Matrimony.com Limited vs. Google LLC & Ors. Case No. 7 of 201222; Paras 249, 196-200)

(WhatsApp v Competition Commission, 2025, para. 54).”

It was further observed by the Tribunal that:

“Furthermore, due to data’s scalable and reusable nature, dominant platforms can reinforce their position by creating high entry barriers, limiting rivals’ access to essential data, and shaping market dynamics in their favour ultimately distorting fair competition... It was brought to our notice that non-price parameters of competition like quality, customer service, and innovation are also valued by users at par with privacy and competition regulators across the world recognise it as a critical non-price parameter of competition. If there is a loss of privacy it is considered as reduction in quality of services. Thus, excessive data collection (with same level of services) amounts to degradation of quality of services and this has been noted in para 182.6 @pg. 108 of Impugned Order”

(WhatsApp v Competition Commission, 2025, para. 55).

The Tribunal went further to comment on the matter of non-monetary considerations, noting that:

“We also note that data driven digital networks typically do not rely on monetary consideration or subscriptions to earn revenue and are frequently either free or at a nominal cost with a view to gain maximum subscribers over a period of at the earliest. We don’t find disagreement in the arguments of the Commission that the real value in such nominally free digital services is in the data of the users which can be monetised to full effect by selling to advertisers etc. Therefore, we cannot accept the definition proposed by Appellants, which excludes non-price factors such as privacy from competition analysis. If accepted, this would effectively remove all non-price based digital services from the scrutiny of competition law. We also note that the ubiquity of digital services and their impact on consumers as a whole are perhaps that regulators worldwide have been considering non-price factors such as privacy are valid for competition analysis.”

(WhatsApp v Competition Commission, 2025, para.56).

The reasoning exercised by the Tribunal in this regard is sober and mature. It demonstrates an evolving understanding of competition matters in the digital environment. The Tribunal is spot on in its analysis and we support the notion that non-price-based considerations cannot be excluded from competition law. To this end, the Tribunal went on to note that:

“We find that the Competition Commission’s authority extends to digital markets where services are provided at zero price, as the real value lies in the data collected from users. The Commission’s scrutiny is not limited to price-based competition but includes non-price factors such as privacy, quality, and innovation, which are critical in digital markets. The scalable and reusable nature of data allows dominant platforms to reinforce their market position, create entry barriers, and distort fair competition, making it imperative for the Commission to intervene”

(WhatsApp v Competition Commission, 2025, para. 59).

Importantly, the Tribunal also went further to provide the legal basis for its findings noting that:

“Furthermore, we find that the legislative framework, including Section 4(2)(a)(i) and Section 4(2)(a)(ii) of the Competition Act, is deliberately broad to capture all forms of abusive conduct, including those involving non-price factors. The Competition Law Review Committee’s findings further support the Commission’s approach, affirming that the Act’s definitions are inclusive enough to encompass data and network effects without requiring amendment. Excluding non-price factors from competition analysis would undermine the Act’s purpose and leave digital markets unregulated, contrary to global regulatory consensus. Therefore, the Competition Commission’s actions in zero-price markets are fully justified and in line with the Act’s spirit and international best practices. We were also clarified that same dominance assessment test applies equally to all markets, whether zero-price markets or non-zero priced markets. We were reminded that consumers pay via their data in zero price markets”

WhatsApp v Competition Commission para 60 – 61. The order of the Tribunal is available in para 264 of the matter.

In our view, this is perhaps the most instrumental part of this judgment. This is because it demonstrates an important piece of understanding with respect to the matter of data-related competition issues that existing principles and definitions are adequate in dealing with issues such as non-price harm. This was in line with the spirit of the Indian Competition Act as well as international best practice. While the amendment of the Act to deliberately include these issues would improve certainty and transparency in relation to the Act, it is important to note that this is not entirely a necessity. Noting that the approach to abuse of dominance in the Indian context is vastly similar to that in the South African Competition Act, parallels can be drawn to the effect that there is therefore no need to amend the Competition Act in South Africa in order to deal with non-price harm with respect to conduct such as excessive data leveraging and excessive data collection.

For example, in Germany, the legislature has adapted the provisions pertaining to dominance in line with the digital environment. For instance, s 18(3) of the German Competition Act provides for how market power is determined, with considerations relevant for data leveraging and collection included (Competition Act 89 of 1998, s. 18(3)(3)). As another example, s 18(3) of the German Competition Act provides access to relevant data for competition as a factor in determining the market position of a firm. Furthermore, s 18(3a) provides a specific market position assessment for multi-sided markets and platforms. Section 18(4) of the German Competition Act goes further to state that, when assessing the market position of an undertaking that serves as an intermediary on multi-side markets, the importance of the intermediary service provided by the undertaking for assessing supply and sales market has to be considered. The inclusion of these provisions in relation to the abuse of dominant position assessments in the South African context would be useful in

dealing with such matters, however, as observed above, they are not entirely necessary as existing rules are adequate to be interpreted to include such harms.

5.5 *Meta Platforms Inc. and Ors v Bundeskartellamt*

Taking on from the discussion above, it becomes important for us to engage the jurisprudence that is emerging from the German side where significant developments have been made in relation to excessive data collection and leveraging in the digital economy. A vital case in this regard is the matter of Meta Platforms Inc. and Ors v Bundeskartellamt Case C-252/21 that was finalised on the 4th of July 2023, which was the final case in the series of matters on this issue. This case has garnered world-wide attention, widely cited as one of the most influential cases on this particular matter. In order to properly contextualise the matter, we first present a chronological order.

The first decision in the matter was taken by the Bundeskartellamt on the 6th of February 2019 (Case B6-22/16). In this matter, the Bundeskartellamt prohibited Facebook Inc. (now Meta Platforms Inc.) from utilising business terms conditioned the use of Facebook to a combination of data collected while using other group-owned services or third-party websites and apps with Facebook user accounts. In a sense therefore, there was a combination of off-Facebook data with on-Facebook data. The Bundeskartellamt prohibited this combination of data from different sources, that was not accompanied by user voluntary consent. Accordingly, this decision had wide-ranging implications on Facebook's ability to process user data.

In its view, Facebook had violated competition regulations by abusing its dominant position by conditioning the use of its social network on the unconditional collection of various user data from third party sources, which would be combined with Facebook's user accounts. Thus, Facebook was collecting data from users from its applications such as Instagram and WhatsApp together with third party websites and applications. The Bundeskartellamt reasoned that a firm in a dominant position such as Facebook could not extensively collect data in this fashion without express voluntary consent. This was also partly because of the fact that the underlying process itself was in violation of the General Data Protection Regulation (GDPR). The position of the Bundeskartellamt was therefore that consumers had to be offered genuine choice in relation to their on-Facebook and off-Facebook data.

Following this decision by the Bundeskartellamt, Meta lodged an appeal. Accordingly, the matter was referred to the Düsseldorf Higher Regional Court (OLG Düsseldorf). On the 26th of August 2019, an interim suspension was granted in favour of Facebook's appeal. This decision was underpinned by the fact that the court was critical of the fact whether a national competition commission could vest their abuse of dominance finding on a breach of the GDPR. Furthermore, the nexus between dominance and the alleged exploitative conduct was questioned. Unfortunately, however, this decision was short-lived.

On 23 June 2020, at the behest of the Bundeskartellamt, the Federal Court of Justice (BGH) considered the Bundeskartellamt's decision concerning Facebook's data-processing practices. Following this, on the 24th of March 2021, the Düsseldorf Higher Regional Court referred some aspects of the matter to the Court of Justice of the European Union (CJEU), which, inter alia, was supposed to deliberate on whether the GDPR could be utilised in considering competition law questions. On the 4th of July 2023, the European Court of Justice (ECJ) ruled in favour of this approach (case C-252/21). To its mind, a national competition authority could examine whether an undertaking's conduct complied with the GDPR as part of assessing abuse of dominance under Article 102 of the Treaty on the Functioning of the European Union (TFEU). This is despite the fact that decisions pertaining to the GDPR are also dealt with separately by another supervisory authority, which could potentially lead to conflicting decisions. To this end, it was noted that consent to data processing had to be freely given.

Further to this, it was also necessary to observe that the existence of a dominant position as a critical factor in assessing whether consent was freely given. On the 10th of October 2024, the final matter in these cases was dispensed with by the Bundeskartellamt. The matter was closed by agreement rather than by judgement. Hereafter, the remedial measures were implemented by Meta, which included the establishment of an Accounts Centre, which provided users with control over cross-service data linking, as well as cookie-consent settings for Business Tools Data and Facebook Login. These measures allow a customer to make a free and informed choice with reference to their data. Subsequently, Meta withdrew its outstanding 2019 OLG Düsseldorf, thus making the 2019 prohibition decision final and binding. This however did not resolve all competition concerns. Commenting on this process, Mundt (2024), then President of the Bundeskartellamt, observed that:

“Our 2019 Facebook decision can still be considered groundbreaking today. As a result of our decision, Meta has made very significant changes to the way it handles user data. The main change is that using the Facebook service no longer requires users to consent to Meta collecting a limitless amount of data and linking such data to their user accounts, even if these data are not even generated while using Facebook. This applies to Meta services such as Instagram or third-party websites and apps. This means that users now have much greater control over how their data are combined. In addition to these very concrete improvements, the Bundeskartellamt’s decision has also led to an important landmark ruling by the Court of Justice of the European Union and has inspired legislative initiatives at both national and European level. This also means that the situation in terms of legal clarity and the instruments available to us to intervene in this area is very different today than it was five years ago.”

He highlights the importance of this contribution in inspiring legislative initiatives at both national and European level. The proceedings also demonstrated the need for collaboration between competition and data protection authorities, as they had to regularly exchange views during the proceedings. Further cooperation was also required from other organisations such as those dealing with consumer protection and information security. It is further anticipated that stricter standards could be set in terms of s 19(a) of the German Competition Act or in terms of provisions of the Digital Markets Act.

What is important from these cases, and perhaps disputed, is the German authority’s assessment that this was a case of exploitative abuse. Herein, Facebook, as a dominant firm had utilised exploitative practices to the detriment of consumers. This exploitative practice was also exclusionary in the sense that it also affected competitors that were not in a position to amass such a treasure trove of data. This accorded with the approach that not only excessive prices could be deemed as exclusionary, but any inappropriate contractual terms and conditions could constitute exploitative abuse (exploitative business terms). Such a business will exploit its market power gained through its dominant position in order to enhance its competitive advantages in a manner that is unlawful and increases barriers to entry. Thus, in our view, it is evident from this case that Meta’s conduct raises both exploitative and exclusionary consequences. Exploitative harm’s which are mostly raised in the case are however difficult to deal with as the authorities in the European Union have prioritised exclusionary abuses. This is largely because of the fact that the difficulty in setting fair price benchmarks. They are thus difficult to prove and require continuous price or term regulation. In a sense, authorities also avoid serving as price regulators. This is in contradistinction to exclusionary conduct that is frequently considered, especially if it relates to the reduction in consumer autonomy.

6. Developing the Framework to Assess Data-Driven Abuse of Dominance in South Africa

The preceding sections illustrate that South Africa’s abuse of dominance jurisprudence has largely been grounded in price-based and foreclosure-based conceptions of harm, notwithstanding the contemporary

reality that data functions both as a mechanism for extracting consumer value (Krafft et al., 2021) and as a key input in the accumulation of market power within the digital economy (Graef, 2015). The main limitation does not lie in the wording of the Competition Act itself, but rather in the courts' reluctance to extend its application to its full potential (Klaasen, 2017). In this section, we propose an interpretive framework through which the Competition Commission may assess excessive data collection and leveraging, under South Africa's abuse of dominance framework without legislative amendment. The proposed framework proceeds with a distinction between data collection as a form of non-monetary extraction from users (Just, 2026) and data leveraging as a mechanism through which dominance or market power may be entrenched or leveraged by platforms operating in multi-sided markets (Vandendriessche & Buts, 2026).

Assessing data as a non-price parameter of Competition Law:

Step 1: Excessive data collection as an exploitative abuse or an exclusionary abuse

The inquiry should commence with the following legal question: does the collection of data strengthen the position of the dominant firm in an adjacent market where competitors are unable to access such data? For certainty, the enquiry must then also consider the question: in circumstances of dominance and the absence of user choice, is the quantity and intrusive data collected disproportionate to what is objectively necessary for the provision of the service?

In this leg of the inquiry, the Regulator treats data as a non-price trading condition imposed on users (Abate et al., 2024). In the digital economy, where services are provided on a zero-price basis (OECD, 2018), dominant operators can condition access to essential or unavoidable services, on the basis of users surrendering extensive personal or behavioural data (Esayas, 2018). In this transaction between the user and the platform, the user pays through the surrender of their data as opposed to a monetary payment (Just, 2026). This paper has found that excessive data collection can be constitutive of exploitative abuse (Scharf, 2022) enshrined in section 8(1)(a) of the Competition Act, specifically where the user is subjected to take-it-or-leave-it terms, where consent is not voluntary or as previously argued, the scope of the collection exceeds the threshold of what constitutes necessary for the provision of the service. To define the harm, it is therefore consumer-facing, as users' privacy and informational autonomy erode, while service choice and quality diminish once they opt to interface with the platform (Esayas, 2018).

When it comes to assessing what constitutes "disproportionality", the Regulator's assessment must be guided by the principles contained in POPIA (see the principles of processing limitation, purpose specification, data minimisation and further processing limitation), which would function as contextual benchmarks to determine whether the extent of data extraction exceeds what is reasonably necessary for the stated purpose of the service (Abate et al., 2024). Similarly, consent as an indicator of quality, together with the existence of meaningful user choice, should assist in assessing whether the extraction conditions imposed by the dominant firm amount to exploitative conditions that users cannot realistically avoid in a contestable market.

This proposed framework does not collapse competition law into data protection regulations. Rather, the data protection provisions act as a contextual benchmark for assessing proportionality, necessity and reasonable expectations within abuse of dominance analysis. Competition law retains its autonomous inquiry focused on dominance and competitive harm, while POPIA assists in determining whether the collection of the data in fact exceeds legitimate commercial justification (European Data Protection Board, 2025, pp. 4–5; May et al., 2023).

Step 2: Excessive data leveraging as an exclusionary or leveraging abuse

At this stage of the inquiry, the Regulator then needs to answer the following legal question: is the data collected subsequently aggregated and shared in a manner that entrenches dominance, forecloses rivals or leverages market power into the adjacent market beyond what is objectively justified?

Where these competitive advantages distort or impede competition or create ground for a dominant firm to leverage its position into an adjacent market, excessive data leveraging has the potential to give rise to exclusionary abuse under section 8(1)(c) or section 8(1)(d), in the alternative. In this stage of the inquiry, the harm is focussed on market foreclosure, affecting market entry, innovation and prospects of rival scalability (Motta, 2022).

A firm's compliance with data protection law does not preclude a finding of exclusionary abuse (Alvarez & Marsal, 2020). Even in the instance that users consent to leveraging practices, competition law may intervene where such a conduct has the ability to distort competitive market conditions, entrench dominance or foreclose effective competition [a distinction must be made between this and information exchange which triggers s 4 of the Competition Act].

Integrating the framework into South Africa's abuse of dominance doctrine

We argue that the proposed framework does not require legislative amendment to the Competition Act (Koornhof, 2021). We take that South Africa's abuse of dominance framework is already sufficiently broad to recognise non-price forms of exploitative and exclusionary abuses (Basson, 2022). The principal limitation is not with the statutory language in and of itself, rather competition practitioners must adapt existing analytical tools to digital markets in which data functions in tandem (Samuel, 2026), both as a form of consideration and as a strategic competitive input. In summary, the two considerations are as follows:

Stage	Legal Focus	Key Question	Type of Abuse	Primary Harm
Step 1	Excessive Data Collection	Is the data collected disproportionate to what is objectively necessary for the provision of the service, or does it strengthen the dominant firm's position in an adjacent market that competitors cannot access?	Exploitative (non-price form) or exclusionary	Users
Step 2	Excessive Data Leveraging	Is the collected data subsequently aggregated or leveraged in a manner that entrenches dominance, forecloses rivals or extends market power into an adjacent market beyond what is objectively justified?	Exclusionary or leveraging	Market structure and competitive dynamics



7. Conclusion

Digital markets have changed the way market power is exercised and the way consumer harm manifests. In many digital markets, dominant firms do not extract value through monetary prices but through the collection, processing, and strategic use of personal data. Traditional competition law tools were developed for markets characterised by price-based transactions and tangible inputs. As a result, they can appear ill-suited to address the realities of data-driven business models. This paper has argued, however, that the challenge is not one of legislative inadequacy. Rather, it lies in the interpretation and application of existing legal provisions. South Africa's Competition Act 89 of 1998 already contains the conceptual foundations necessary to address data-driven harm without requiring legislative amendment.

To this end, a two-step interpretive framework is proposed in this paper. The first step focuses on excessive data collection. Drawing on principles of proportionality, necessity, and users' reasonable expectations, and using POPIA as an important contextual benchmark, excessive data collection may constitute exploitative abuse where users are subjected to take-it-or-leave-it terms and are deprived of meaningful choice. The second step focuses on excessive data leveraging and aggregation. Here, the assessment turns to the effects of data practices on rival scalability, barriers to entry, and the leveraging of market power across multiple markets. Where data aggregation strengthens dominance or forecloses effective competition, exclusionary or leveraging abuse may arise. Although related, these two inquiries remain analytically distinct. The first addresses harm experienced by users, while the second concerns the impact on market structure and competitive processes.

Comparative developments in India provide further support for this approach. The progression from the Competition Commission of India's 2021 Suo motu proceedings to its 2024 decision against Meta and WhatsApp, together with the affirmation of that decision by the NCLAT in 2025, demonstrates that existing competition law frameworks can effectively address non-price digital harms without legislative reform. Particularly significant is the recognition by Indian authorities and courts that privacy can function as a parameter of competition and that competition law and data protection law operate in a complementary, rather than conflicting, manner. These developments offer persuasive guidance for South African adjudicators confronting similar issues.

The Competition Act's prohibition of abuse of dominance is broad enough to capture both non-monetary forms of exploitation and data-driven exclusionary conduct. What is required is not the creation of new legal rules, but a more expansive application of existing ones. Such an approach would recognise data as a form of consideration, privacy degradation as a reduction in quality, and data aggregation as a source of market power. This paper has sought to provide the interpretive basis for that development. The South African Competition Commission is well placed to advance this jurisprudence by drawing on the framework proposed here, the comparative lessons emerging from other jurisdictions, and the growing international consensus regarding the competitive significance of data in digital markets.

8. References

Cases — South Africa

American Natural Soda Ash Corporation and Another v Competition Commission of South Africa 2005 (6) SA 158 (SCA).

Competition Commission and South African Airways (Pty) Ltd [2005] ZACT 50.

Competition Commission v Media 24 (Pty) Ltd [2018] ZACAC 1.

Competition Commission v Senwes Ltd 110/CR/Dec06; 110/CAC/Dec10.

Competition Commission v South African Airways (Pty) Ltd 2011 (3) SA 76 (CC).

Competition Commission of South Africa v Media 24 2019 (5) SA 598 (CC).

Harmony Gold Mining Company Ltd v Mittal Steel South Africa Ltd [2009] ZACAC 1.

Media24 (Pty) Ltd v Competition Commission 2016 (5) SA 151 (SCA).

Nationwide Poles and Sasol (Oil) Pty Ltd (72/CR/Dec03) [2005] ZACT 17; [2005] 1 CPLR 156 (CT).

Sasol Chemical Industries Ltd v Competition Commission 2015 ZACAC 4; 2015 (5) SA 471 (CAC).

Cases — India

In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users Suo Moto Case No. 1 of 2021 (Competition Commission of India).

K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC (Supreme Court of India).

Karmanya Singh Sareen v Union of India W.P. (C) 7663 of 2016 (Delhi High Court).

Karmanya Sareen v Union of India SLP (C) No. 804 of 2017 (Supreme Court of India).

Shri Vinod Kumar Gupta, Chartered v WhatsApp Inc Case No. 99 of 2016 (Competition Commission of India).

Vinod Kumar Gupta v Competition Commission of India Competition Appeal No. (AT) 13 of 2017 (NCLAT).

WhatsApp LLC v Competition Commission and Others Competition Appeal No. 1 of 2025 (NCLAT).

Winzo Games Private Limited v Google LLC and Others Case No. 42 of 2022 (Competition Commission of India).

Legislation — South Africa

Competition Act 89 of 1998 (as amended).

Constitution of the Republic of South Africa, 1996.

Protection of Personal Information Act 4 of 2013 (POPIA).



Legislation — Foreign

Competition Act 2002 (India).

Act Against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB) (Germany).

Digital Personal Data Protection Act 2023 (India).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India).

Secondary Sources

Books, journal articles, theses, reports, and online sources

Aamir, S. (2025). Going digital with multisided-platforms: Assessing the innovation adoption process from the perspectives of travel agents. *Tourism and Hospitality Research*, 25, 72–89.

Abate, C., Bianco, G., & Casalini, F. (2024). The intersection between competition and data privacy. OECD.

Abraham, R. P. (2025). Excessive data collection in an ecosystem as an exploitative and exclusionary abuse: A critical analysis of the CCI's order against WhatsApp's privacy policy and its impact on the digital advertising market. *Yearbook of Antitrust and Regulatory Studies*, 18, 179–194.

Alghamdi, O. A., & Agag, G. (2024). Competitive advantage: A longitudinal analysis of the roles of data-driven innovation capabilities, marketing agility, and market turbulence. *Journal of Retailing and Consumer Services*, 76, 1–15.

Alvarez & Marsal. (n.d.). Impact of competition law on privacy compliance in the data economy. <https://www.alvarezandmarsal.com/insights/impact-competition-law-privacy-compliance-data-economy>

Arestis, P., & Eng, K. Y. (n.d.). The comparative analysis of the economic effects of competition law on the United States and China. <https://doi.org/10.2298/pan250103030a>

Bundeskartellamt Facebook; Umsetzung des Beschlusses vom 6. Februar 2019 (Konditionenmissbrauch wegen unangemessener Datenverarbeitung). <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/07/european-court-of-justice-in-facebook-ruling-clarifies-interplay-between-eu-competition-law-and-data-protections-enforcement.pdf>.

Basson, A. (n.d.). Greater cooperation between regulators needed against abuse of internet dominance. <https://www.su.ac.za/en/faculties/medicine/node/5997>

Centre for Internet and Digital Economy. (n.d.). Economics of data-driven markets – Mitigating market power: Options and trade-offs. <https://icrier.org/pdf/Economics-of-Data-Driven-Markets-Mitigating-Market-Power.pdf>

Choe, C., et al. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, 173, 113–124.

Competition Commission of South Africa. (2021). Competition in the digital economy. <https://www.compcom.co.za/wp-content/uploads/2021/03/Digital-Markets-Paper-2021-002-1.pdf>



Competition Commission of South Africa 'Media and Digital Platforms Market Inquiry' (2022).

Costa-Cabral, F., & Lynskey, O. (2017). Family ties: The intersection between data protection and competition in EU law. *Common Market Law Review*, 54, 11–50.

Crowell 'A New Playbook for M&A in the EU: The European Commission's Draft Merger Guidelines – 10 Key Changes' available at <https://www.crowell.com/en/insights/client-alerts/a-new-playbook-for-manda-in-the-eu-the-european-commissions-draft-merger-guidelines-10-key-changes> (accessed 22 May 2026).

Esayas, S. (n.d.). Privacy as a non-price competition parameter: Theories of harm in mergers. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232701

Esayas, S. Y. (2017). Privacy-as-a-quality parameter: Some reflections on the scepticism. *Stockholm Faculty of Law Research Paper Series*, 43, 1–38.

European Data Protection Board 'Position Paper on Interplay between Data Protection and Competition Law' (2025) available at https://www.edpb.europa.eu/system/files/2025-01/edpb_position-paper_20250116_interplay-between-data-protection-and-competition-law_en.pdf (accessed 2 March 2026).

Fischer, B., & Benjamin, M. (2021). The rise of the data-opoly: Consumer harm in the digital economy. *Washington University Law Review*, 99, 729–750.

Graef, I. (2015). Market definition and market power in data: The case of online platforms. In Rivas et al. (Eds.), *World Competition: Law and Economics Review* (pp. 473–505).

Gumede, S., & Manenzhe, P. (2023). Competition regulation for digital markets: The South African experience. *The African Journal of Information and Communication*, 31, 1–19.

Gupta, G. (2022). Does “big data” provide a competitive advantage to firms: An antitrust analysis. *Asian Journal of Business Ethics*, 11, 423–442.

Haftor, D. M., et al. (2023). A pathway to bypassing market entry barriers from data network effects: A case study of a start-up's use of machine learning. *Journal of Business Research*, 168, 1–18.

Iacobucci, E. M. (2026). Consumer privacy and anticompetitive exclusion. *Journal of Competition Law and Economics*, 22, 138–158.

Janita, M. S., & Miranda, F. J. (2013). Exploring service quality dimensions in B2B e-marketplaces. *Journal of Electronic Commerce Research*, 14, 363–386.

Just, N. (2026). Beyond price and money: From early insights to contemporary theorising of non-price competition and non-monetary exchange in internet markets. *Telecommunications Policy*, 50, 103–167.

Kathuria, V., & Globocnik, J. (2019). Exclusionary conduct in data-driven markets: Limitations of data sharing remedy. *Journal of Antitrust Enforcement*, 511–534.

Këllezi, P. (n.d.). Data protection and competition law: Non-compliance as abuse of dominant position. <https://sui-generis.ch/article/view/sg.114/1220>

Klaasen A 'Constitutional Interpretation in the So-Called “Hard Cases”: Revisiting S v Makwanyane' (2017) *De Jure* 1 – 17.



Knapstad, T. (2024). Digital dominance: Assessing market definition and market power for online platforms under Article 102 TFEU. *European Competition Journal*, 20, 412–436.

Konstantopoulou, E. S. (2026). Building a single market for data: Data spaces as pro-competitive infrastructure. *Data in Brief*, 1–38.

Koornhof, P. G. J. (2021). Abuse of dominance and the internet: An assessment of the South African regulatory framework (Unpublished LLD thesis). Stellenbosch University.

Krafft, M. F., et al. (2021). Insight is power: Understanding the terms of the consumer-firm data exchange. *Journal of Retailing*, 97, 133–149.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38, 1134–1145.

Li, Q., & Cauffman, C. (2025). Abuse of relative dominance by digital platforms: A law and economics perspective. *GRUR International*, 74, 217–225.

Li, W. C., Nirei, M., & Yamana, K. (2019). Value of data: There's no such thing as a free lunch in the digital economy. RIETI.

May et al 'Competition in the Digital Age: Can Breaching Data Privacy Laws also Infringe Competition Law?' available at

<https://www.cliffedekkerhofmeyr.com/en/news/publications/2023/Practice/Competition/combined-competition-and-tmt-alert-2-august-competition-in-the-digital-age> (accessed 21 May 2026).

Motta, M. (n.d.). Self-preferencing and foreclosure in digital markets: Theories of harm for abuse cases. https://bse.eu/sites/default/files/working_paper_pdfs/1374_0.pdf

Nayal, R. (2022). Data privacy at the altar of competition laws. *Journal on Competition Law and Policy*, 3, 79–95.

Nxumalo, M. (n.d.). Fruit from the neighbour's tree: On indirect extra-territorial effects of South Africa's competition law rulings. <https://www.compcom.co.za/wp-content/uploads/2014/09/Fruit-From-The-Neighbours-Tree-Final.pdf>

O'Callaghan, P. (2018). The intersection between data protection and competition law: How to incorporate data protection, as a non-economic objective, into EU competition analysis. *Trinity College Law Review*, 21, 109–136.

OECD. (2018). Quality considerations in digital zero-price markets. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/03/quality-considerations-in-the-zero-price-economy_85631bda/8022ca46-en.pdf

OECD. (2024). The impact of data portability on user empowerment, innovation, and competition. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf

Padilla, J. (n.d.). What is an exclusionary abuse? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5006000



Patakyova, M. T. (2020). Competition law in digital era – How to define the relevant market? In Proceedings of EMAN 2020: Economics & Management: How to cope with disrupted times. Association of Economists and Management of the Balkans.

Pavlidou S 'Quality Considerations in Digital Zero-Price Markets' available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3862529 (accessed 6 May 2026).

Rahman, N. A., & Setyawati, R. (2026). The interface between competition law and data protection: The need for a more integrated approach. *Media Iuris*, 1, 181–212.

Rautenbach C 'The Influence of Foreign Judgments on The Development of Post-Apartheid Constitutional Law in South Africa: Judicial Law-Making in Action?' (2020) 7 *JICL* 99 – 126.

Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, 57, 161–190.

Rudman D and Ostrovsky S 'Dominance Test: A Superfluous Jurisdictional Hurdle?' available at <https://www.compcom.co.za/wp-content/uploads/2014/09/article-dominance-test.pdf> (accessed 23 May 2026).

Samuel, O. A. (n.d.). From SSNIP to SSNDQ: Adapting competition analysis tools for zero-price digital markets in developing economies: Lessons from Nigeria's FCCPC. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6447338

Scharf, A. (2022). Excessive data collection as abuse of dominance under Art 102 TFEU. *University of Vienna Law Review*, 6, 141–198.

Shaiek, E. F. (n.d.). Excessive data collection as an abuse of dominant position: The implications of the digital data era on EU competition law and policy. <https://www.diva-portal.org/smash/get/diva2:1581861/FULLTEXT01.pdf>

Shah, M., & Tomar, A. S. (2022). Why WhatsApp is no more a consensual way of saying wassup: A saga of WhatsApp privacy policy under Indian competition act. *Lex Humana, Petrópolis*, 14, 1–22.

Taufiqurrohman, et al. (2025). Digital markets and data exploitation: Addressing abuse of dominance under Indonesian competition law. *Jurnal Penelitian Hukum De Jure*, 25, 1–18.

van der Waerdt, P. (2025). Reinforcing data protection and competition through Art. 6(2) of the Digital Markets Act. *International Review of Law & Economics*, 82, 1–17.

Vandendriessche, R., & Buts, C. (2026). Data-derived market power: Toward a data ecosystem approach in merger control. *Journal of Competition Law and Economics*, 1–30.