

Assessing a Digital Platform's Personal Data Processing Terms of Use as a Competition Law Violation.

Vellah Kedogo Kigwiru

ABSTRACT

In 2019, the German Bundeskartellamt took a bold step, becoming the first competition agency in the world to consider a data breach a competition law violation by prohibiting Facebook from combining data from third-party websites and its own platforms (WhatsApp and Instagram) without users' voluntary consent. It is now widely recognized that the 2019 Bundeskartellamt/Facebook decision influenced the EU Digital Markets Act (DMA) data-related prohibitions and investigations by competition agencies in Argentina, Brazil, Chile, India, and Nigeria into Meta's data processing terms of use regarding consent. In light of the novelty and influence of the Bundeskartellamt/Facebook decision, considerable academic research has focused primarily on whether a causal link exists between competition and data protection law, warranting investigation by a competition agency. This paper argues that instead of focusing on a data breach which raises questions on regulatory intrusion, competition agencies should adopt a competition-oriented approach focusing on data as a source of a firm's dominance, whether the alleged conduct is prohibited under competition law and leads to a competition harm that meets the causality requirement as required under competition law, regardless of whether the same conduct is prohibited under another regulatory framework. This approach, if adopted, views a data breach as a source of, and as vital evidence of, a competition law violation, thereby minimizing the likelihood of jurisdictional conflicts, conflicts of law, legal uncertainty, and conflicting decisions between a data protection and a competition agency. To support this claim, in addition to the Bundeskartellamt, this paper analyzes the interpretations of two German courts (the Oberlandesgericht and the Bundesgerichtshof) and the Court of Justice of the European Union (CJEU) in the context of the Bundeskartellamt/Facebook case revealing how the four institutions assessed Facebook's data processing terms of use to provide lessons for other competition agencies likely to assess similar regulatory challenges.

1.0 Introduction

Facebook is an online social networking platform that enables users to connect with friends and family and share content such as text, photos, and videos. Facebook was launched on February 4, 2004, by Mark Zuckerberg and his classmates Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes at Harvard University. Facebook later acquired Instagram in 2012 and WhatsApp in 2014, respectively. In 2021, Facebook changed its name to Meta, which now serves as the parent company of Facebook, WhatsApp, Instagram, Meta AI, Messenger, Meta Quest, Meta Horizon, and Threads.¹

To access and use Facebook, users create a Facebook account and set up a user profile by providing their personal data.² In addition to collecting personal data from users' direct interactions on Facebook (known as first-party tracking), Facebook also collects user data outside its social network (known as third-party tracking) by using its application programming interfaces (APIs), such as the Facebook Business Tool, storage technologies, and cookies, which are integrated into users' devices, including laptops, smartphones, and tablets. According to Zuckerberg, the data collected is solely for operating its social networking service.³ Facebook also argues that it gives people control over their personal data by seeking their consent to process it for a personalized experience and targeted advertising.⁴

Despite Facebook's assertion that it obtains users' consent to the processing of their data, the question of whether users give consent to Facebook's processing of their personal data by clicking "I Agree" has been contentious for a long time.⁵ For instance, Srinivasan argues that the social network market has consolidated towards Facebook and 'consumers effectively face a singular choice—use Facebook and submit to the quality and stipulations of Facebook's product or forgo all the use of the only social network used by most of their friends, family, and acquaintances'.⁶ Accordingly, because user consent is the price users pay to participate and access social infrastructures like Facebook, consent in digital markets has been termed as

¹ Meta, 'Our History' Available here <https://www.meta.com/en-gb/about/company-info/> accessed 29 September 2025.

² Personal data generally refers to any information that is connected directly or indirectly to a person, and which can identify that person, such as their name, home address, sexual orientation, or ethnic background, among others.

³ See Mark Zuckerberg, 'Understanding Facebook's Business Model' (Meta, 24 Jan 2019) Available at <https://about.fb.com/news/2019/01/understanding-facebooks-business-model/> accessed 12 March 2025.

⁴ Facebook, 'The Best Person to Be in Control of Data is You' Available at <https://www.facebook.com/off-facebook-activity> accessed 15 October 2025.

⁵ Rikke Frank Joergensen, 'The Unbearable Lightness of User Consent' (2014) 3(4) Internet Policy Review 1.

⁶ Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumer's Preference for Privacy' (2019) 16(1) Berkeley Business Law Journal, 40.

an illusion and an empty construct.⁷ In Koop's view, consent is largely 'theoretical and has no practical meaning', especially in the internet-based services where 'most people just tick consent boxes without reading or understanding privacy statements'.⁸

Generally, the lack of valid consent in the processing of personal data is investigated and enforced by data protection agencies.⁹ In recent years, however, competition agencies have begun to consider the lack of valid user consent in the processing of personal data by digital platforms as a potential violation of competition law. The German Bundeskartellamt, the agency responsible for enforcing Germany's Act Against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen-GWB), is the first competition agency to find a lack of valid consent for the processing of personal data by a digital platform to constitute a competition law violation. Following an investigation, on 6 February 2019, the Bundeskartellamt prohibited Facebook from combining user data from third-party websites, apps, and its own services, including Instagram and WhatsApp.¹⁰ The Bundeskartellamt found that Facebook's conduct constituted an exploitative abuse in contravention of Article 19(a) of the GWB.

The Bundeskartellamt further stated that Facebook's conduct also violated the 2018 European Union (EU) General Data Protection Regulation (GDPR). In particular, Facebook breached Article 4(11) of the GDPR which provides that consent of the data subject means any 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. In the Bundeskartellamt's view, there was 'no effective consent to the user's information being collected if their consent is a prerequisite for using the Facebook.com service in the first place'.¹¹ By recognizing that a data breach constituted an exploitative conduct prohibited under competition law, the Bundeskartellamt became the first competition agency in the world to do so.

Since the 2019 Bundeskartellamt/Facebook decision, considerable attention has been devoted to whether there is a causal link between data protection and competition law to

⁷ Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250.

⁸ Ibid at 251.

⁹ In addition to valid consent, data controller may process the personal information of the data subject when it is necessary for the performance of a contract, in compliance with a legal obligation, to protect the vital interests of the data subject, to pursue a public interest, or to protect legitimate interests.

¹⁰ Bundeskartellamt, Case B6-22/16 at 1.

¹¹ Ibid.

warrant a competition agency investigation.¹² Those supporting the integration of data breaches into competition law analysis argue that access to and control over data entrench tech companies' market dominance, creating a conducive environment for them to abuse their dominant position, as prohibited under competition law.¹³ Thus, competition agencies can use a violation of data protection law as a metric of market dominance in investigating the abuse of a dominant position by digital platforms.¹⁴

To critics, competition law intervention in data regulation is premature, misguided, introduces subjectivity, and hinders innovation.¹⁵ Additionally, critics note that data protection and competition law address distinct types of harm.¹⁶ Data protection aims to protect individuals from privacy harm, strengthening their autonomy and dignity. Competition law, on the other hand, seeks to facilitate the market's competitive process by prohibiting companies' conduct that negatively affects product prices, quality, and innovation, thereby enhancing consumer welfare and economic competition. Furthermore, if competition agencies consider data protection breaches, it is likely to conflate two fields of enquiry and lead to jurisdictional complexities. Thus, it is essential to maintain clear boundaries between data protection and competition law enforcement in digital markets.¹⁷

Regardless of one's stance on the debate, as will be further clarified in this paper, the Bundeskartellamt/Facebook decision has reemphasized the role of data in the digital economy and reflects a shift by competition agencies to expand their scope of inquiry into considering data protection in competition law analysis. The emerging scholarly work on the intersection between data and competition law, however, has focused on demonstrating whether a breach of data protection law can constitute a violation of competition law. Framing this discussion in this way shifts focus to a data breach, which is a concern for the data protection agency and

¹² Recent books on the interplay between data protection and competition law include: Maria Ioannidou and Despoina Mantzari, *Research Handbook on Data Privacy and Competition Law* (Edward Elgar Publishing 2025); Samson Y Esayas, *Data Privacy and Competition Law in the Age of Big Data: Unpacking the Interface Through Complexity Science* (Oxford University Press 2024); Arletta Gorecka, *The Interface between Competition Law and Data Privacy Law: Violations of Privacy as an Exploitative Theory of Harm under Article 102 TFEU* (Springer 2024).

¹³ Klaudia Majcher, *Coherence Between Data Protection and Competition Law* (Oxford University Press 2023).

¹⁴ Arletta Gorecka, 'On the Interplay between Competition Law and Privacy: The Impact of Meta Platforms Case' (2024) 20(3) *European Competition Journal* 555; Carolina Abate, Giuseppe Bianco and Francesca Casalini, 'The Intersection Between Competition and Data Privacy' (OECD 2024).

¹⁵ D Daniel Sokol and Roisin E Comerford, 'Antitrust and Regulating Big Data' (2016) 23 *Geo. Mason L. Rev.* 1129.

¹⁶ Inge Graef and Bart van der Sloot, 'Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving beyond Individual Empowerment' (2022) 33(4) *European Business Law Review* 513; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition Consumer Protection, and the Right (Approach) to Privacy' (2015) 80 *Antitrust Law Journal* 121.

¹⁷ Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: Intersection Between Data Protection and Competition in EU Law' (2017) 54(1) *Common Market Law Review* 12.

raises eyebrows, as some policymakers may think the competition agency is investigating conduct outside its jurisdiction, thereby exacerbating jurisdictional conflicts. It also places an obligation on competition agencies to first determine whether a data breach occurred and then to demonstrate whether it led to a competition law violation.

Instead of demonstrating whether there is a causal relationship between data protection and competition law, this paper shifts the focus of competition agencies to determining whether the data processing terms of use of digital platforms raise concerns under competition law. Rephrasing this discussion in this way shifts the focus of competition agencies from a data breach under a data protection legislation to the digital platforms' conduct as it relates to the data processing terms of use. Consequently, a competition agency takes a competition-oriented approach to investigating data processing terms of use, which becomes a competition law concern because these terms strengthen the digital dominant position through data power. Data power, as defined by Lynskey, is 'a multi-faceted form of power stemming from a company's control of data flows'.¹⁸ The more a platform has data power, the more likely it is to access, analyze, and control data flows, thereby granting it a competitive advantage. And because data power can have a significant impact on a digital platform's dominant position, it is a concern for competition law, which is concerned with firms' abuse of market power.¹⁹ Moreover, the digital platform's data processing terms of use lead to conduct prohibited under competition law, the conduct meets the legal test required to prove it under competition law, and results in competition harm. Finally, there is a causal link between the anti-competitive conduct and the resulting harm as required under competition law.

To support a competition-oriented approach to analyzing a digital platform's data processing terms of use, which would also constitute a data breach under a data protection legislation like the GDPR, this paper examines the 2019 Bundeskartellamt/Facebook case, from the Bundeskartellamt's decision on 6 February 2019 to the Court of Justice of the European Union's (CJEU) decision on 4 July 2023. Facebook appealed the Bundeskartellamt's decision to the Oberlandesgericht, Düsseldorf (Higher Regional Court, OLG). The OLG suspended the Bundeskartellamt decision. The Bundeskartellamt appealed the OLG decision to the Bundesgerichtshof, the German Federal Court of Justice (FCJ), which ruled in its favour. After the FCJ decision, the OLG referred seven preliminary questions to the CJEU for

¹⁸ Orla Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 *Theoretical Inquiries in Law* 189, 196.

¹⁹ Tone Knapstad, 'Digital Dominance: Assessing Market Definition and Market Power for Online Platforms under Article 102 TFEU' (2024) 20 (2) *European Competition Journal* 412.

interpretation, including one on whether a competition agency can consider a data breach when investigating a competition law violation. The CJEU made its decision on 4 July 2023, in favour of the Bundeskartellamt's decision. While the FCJ and CJEU agreed with the Bundeskartellamt that Facebook's data processing terms of use constituted an abuse of its dominant position, there are some variations in interpretations. For instance, unlike the Bundeskartellamt, which focused on linking a data breach to Facebook's abuse of dominant position, the FCJ and the CJEU took a competition-oriented approach, focusing on the anti-competitive effects of Facebook's conduct as required under competition law. Thus, this conflicting institutional analysis provides a prism through which we can examine when a digital platform's data processing terms become a concern under competition law.

This paper is the first to provide an in-depth analysis of the Bundeskartellamt/Facebook case by examining the decisions of the Bundeskartellamt, the OLG, the FCJ, and the CJEU. In addition to making a scholarly contribution to the emerging research on the nexus between data protection and competition law, this work also discusses important elements of competition assessment as they relate to data processing terms of use. For example, how the four institutions identified data as a metric of market power, how they developed a competition-harm framework from a privacy-harm framework, and how they established a causal requirement in the context of abuse of dominant position relating to data. In this paper, I use the terms consumers, users, and data subjects interchangeably, as they are used differently in competition and data protection law. But refer to the same subjects who access and use digital platforms.

The rest of the paper proceeds as follows. As the Bundeskartellamt/Facebook decision identified a data breach due to a lack of valid consent, Section two discusses the concept of consent and the elements of valid consent in data protection law, providing a deeper understanding for competition agencies. Section three adopts a competition-oriented approach to demonstrate how the data processing terms of use of digital platforms, as they relate to user consent, can constitute an anti-competitive conduct. Section four makes an empirical contribution by assessing the Bundeskartellamt/Facebook decision to identify how Facebook's conduct of requiring user consent to combine data from its social network with personal data collected on Facebook, on conditional use of Facebook, was interpreted by the Bundeskartellamt, OLG, FCJ, and the CJEU as a competition issue. Section five discusses the findings and provides a roadmap for how and when competition agencies can treat a digital platform's data processing terms of use as a competition law concern within their jurisdiction without raising jurisdictional conflicts with data protection agencies.

2.0 The Concept of Consent in Data Protection Law

2.1 Defining consent in data protection law.

The Bundeskartellamt argued that Facebook's conduct that required users to provide consent to Facebook to combine on-Facebook and off-Facebook data from third parties on conditional use of Facebook constituted a lack of valid consent in contrast to Article 4(11) of the GDPR. In doing so, Facebook abused its dominant position in contravention of Section 19(1) GWB. Before analyzing whether a lack of valid consent in the processing of personal data constitutes a competition law violation, competition agencies need to understand the concept of consent.

Even though the term consent is ubiquitous in our daily lives and has a legitimating function or value that 'serves important social and normative functions in our society,' the concept of consent lacks a single definition and is used differently in various contexts.²⁰ Additionally, consent is 'highly dependent on the social, political, and cultural conditions that enable it: things that amount to consent in one society or group may not amount to consent in other contexts'.²¹ Nonetheless, there are attempts to define what constitutes consent. For instance, in defining consent, the Australian Government, eSafety Commissioner defines consent as the 'informed and freely given agreement to engage in an activity. It involves one person seeking permission from the other before engaging in an activity, and the other person "affirming" or giving their permission for that to happen'.²² Consent, therefore, is intended to empower individuals to exercise their decisional power and determine what information about them is disclosed when, how, and to whom.

In a broader perspective, the concept of consent in data protection law is rooted in the foundational principles of privacy rights that emerged in the mid-20th century. In their seminal article, which laid the foundation for the right to privacy, Warren and Brandeis noted that individuals should enjoy the right to be let alone and that only an individual is entitled to decide which personal information should be made public.²³ Since then, privacy has been conceptualized as a reflection of an individual's freedom and dignity.²⁴

²⁰ Elletta Bietti, 'Consent as a Free Pass: Platform Power and the Limits of Informational Turn' (2020) 40(1) Pace Law Review 310, 317.

²¹ Ibid at 319.

²² eSafety Commissioner, 'Consent' Available at <https://www.esafety.gov.au/key-topics/staying-safe/consent#:~:text=Consent%20is%20the%20informed%20and,permission%20for%20that%20to%20happen>. Accessed 15 June 2025.

²³ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193, 199.

²⁴ James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 (6) The Yale Law Journal 1153.

Dignity refers to our sense of being worthy of respect, which depends on intersubjective norms that define the forms of conduct that constitute respect between persons and determine social interactions.²⁵ That is why, in protecting personal dignity, an individual's personal information relating to their private life cannot be disclosed, especially if it is likely to degrade their standing in their social relations, unless they consent to such disclosure. In the digital world, for instance, an individual has the right to visit various websites privately – even when such websites are not socially accepted – and refuse to have their personal data from visited websites combined across other digital platforms that would reflect their user preferences and undermine the respect accorded to them in their social relations.

The right to privacy is also intended to protect an individual's freedom. In Post's view, privacy as freedom 'imagines persons as autonomous and self-defining, rather than as socially embedded and tied together through common socialization into shared norms'.²⁶ In his classic work on privacy as freedom, Westin asserts that privacy 'provides individuals and groups in society with a preservation of autonomy, a release from role-playing, a time for self-evaluation and for protected communication'.²⁷ When people have control over how their data is processed, they are also exercising their right to self-determination, which proclaims that 'people should have control over what happens with their personal data'.²⁸ From this perspective, privacy as freedom enhances an individual's independence, individuality, and personhood, allowing them to be themselves outside the constraints of social norms.²⁹

It is from the central role of privacy in protecting and strengthening individuals' freedom and dignity during the processing of their personal data that a lack of consent to such processing is considered a privacy harm. To ensure that a person does not suffer from privacy harm, in the EU, before the 2018 EU GDPR, consent was recognized in the 1995 EU Data Protection Directive (DPP), the predecessor of the GDPR.³⁰ The DPP recognized consent in Article 2(h) to mean 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. Consent was also incorporated in the 2000 EU Charter of Fundamental Rights (ECFR, Article 8), which grants everyone the right to the protection of personal data concerning them. Article 8(2) of the

²⁵ Robert C Post, 'Three Concepts of Privacy' (2001) 89 Georgetown Law Journal 2088, 2092.

²⁶ Ibid, at 2095.

²⁷ Alan F Westin, 'Privacy and Freedom' (1968) 25(1) Washington and Lee Review 166, 166.

²⁸ Koops above n7, at 251.

²⁹ Giacomo Pisani, 'The Right to Self-determination in the Digital Platform Economy' (2024) 53 Computer Law & Security Review 1, 5.

³⁰ EU, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

ECFR provides that personal data must be ‘processed fairly for specified purposes and on the basis on the consent of the person concerned or some other legitimate basis laid down by law’.

Instead of defining what consent is, Article 4(11) of the EU GDPR identifies consent to mean any ‘freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’. Article 4(11) of the GDPR has been construed to identify the elements of valid consent and is reflected in most of the data protection legislation enacted worldwide after the GDPR, as seen in Article 6 of the 2023 India Digital Data Protection Act (DDPA),³¹ Article 2 of the Kenyan Data Protection Act,³² and Article 4(11) of the 2016 UK GDPR,³³ among others. The European Data Protection Board (EDPB) Guidelines 05/2020 on consent also identify the elements of consent as being freely given, specific, informed, and an unambiguous indication of the data subject's wishes.³⁴

2.2 Elements of valid consent

It is essential for competition agencies to comprehend the elements of a valid consent, as this can determine whether a digital platform’s data processing terms may lead to exclusionary or exploitative conduct prohibited under competition law, as discussed in Section 3 of this paper. The EU GDPR is the only legislation that expounds in detail the elements of valid consent to the processing of personal data in its recitals. Thus, it should not be surprising if other data protection legislation, especially those modeled after the GDPR, and competition agencies investigating digital platforms’ data processing terms of use as they relate to consent, draw on the EU’s interpretation of elements of valid consent.

a. Freely given

The concept of freely given consent, as outlined in the GDPR and the EDPB,³⁵ implies a voluntary and autonomous choice to accept or decline the processing of personal data. Recital 42 of the GDPR, for example, provides that ‘consent should not be regarded as freely given if

³¹ Article 6 of the India DPPA provides that the ‘consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary’.

³² Article 2 of the Kenyan 2019 Data Protection Act defines consent to mean, ‘any manifestation of express, unequivocal, free, specific and informed indication of the data subject’s wished by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

³³ Article 4(11) of the UK GDPR provides that consent of the data subject means freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

³⁴ EDPB Guidelines 05/2020 on Consent, 7-18.

³⁵ EDPB, ‘Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Model’s Implemented by Large Online Platforms’ (Adopted on 17 April 2024), 19.

the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'. For consent to be freely given, it must be voluntary, without coercion, fraud, undue influence, or any other form of pressure. Under Article 7(4) of the GDPR, when determining whether consent is freely given, 'utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'. Broadly speaking, if consent is obtained through conditional access to and use of a digital platform, and the processing of personal data is not necessary for the performance of a contract or the provision of a digital service, this consent is deemed not to be freely given.³⁶

Another way to infer that consent is freely given is when the user has the right to withdraw their consent at any time. Actually, as noted under Article 7(3) of the GDPR, 'it should be easy to withdraw as to give consent'.³⁷ If the right to withdraw consent is detrimental, that consent cannot be deemed freely given. Detrimental withdrawal of consent to data processing occurs when the digital platform threatens that consumers will not be able to access the service or other services provided by the platform. Or when the digital platform degrades the quality of its services until the consumer consents to the combination of data across the digital platform's other services. For example, poor quality can manifest as numerous cookie consent pop-ups or notifications that become a nuisance to the user or lead to consent fatigue, until they accept the digital platform's terms of use for data processing.

Additionally, the freedom of choice is negated when users have no realistic alternatives to switch to. For example, where a digital platform is dominant, they are likely to 'exploit the situation by forcing the users to accept privacy policies with far-reaching terms regarding the collection and use of their personal data'.³⁸ According to the European Data Protection Supervisor (EDPS) 'where there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory'.³⁹ This problem is well captured by Koops, who notes that in online markets:

Often, there is little to choose: if you want to use a service, you have to comply with the conditions— if you do not click the consent box, access will be denied. And there are no good alternatives: most other providers of the service you want apply the same practice and

³⁶ Alessia Sophia D'Amico, 'Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?' (2023) 8(2) *A Journal on Law and Integration* 611.

³⁷ EU GDPR, Art 7(3).

³⁸ Wolfgang Kerber and Karsten Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2022) 54 *European Journal of Law & Economics* 217, 226

³⁹ EDPS, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (EDPS 2014).

similar data-processing conditions, and with the most-used major services, such as Facebook, Google, or Twitter, there is no realistic alternative for most people.⁴⁰

b. Specific

The element of specific consent requires that consent be obtained for a specific purpose. In cases involving multiple data processing for more than one purpose, separate consent should be obtained for each purpose. The EPBP notes that in such a case, ‘data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes’.⁴¹ Similarly, Recital 32 of the GDPR notes that ‘consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them’. Thus, in cases where a platform offers different services across multiple platforms, such as Meta, which owns Facebook, Instagram, and WhatsApp, competition agencies should examine whether consent for the processing of data on each platform is obtained separately by Meta or bundled together.

c. Informed

The element of informed consent implies that the data subject must be provided with adequate information before their consent is obtained. This enhances transparency and empowers data subjects to exercise control over their data. The EDPB, in its Guidelines 05/2020, notes that the data must provide adequate information to ensure the data subject makes an informed choice regarding whether to give consent or withdraw it. This information includes the controllers’ identity, the purpose of each processing operation for which consent is sought, the data that will be collected and used, and the procedure for withdrawing consent, among other details.⁴²

d. Explicit

Regarding the requirement for an unambiguous indication of wishes, the data subject should provide a statement or take a clear affirmative action to signify their agreement to the processing of their personal data. An ambiguous consent is explicit and clear. Additionally, consent should be provided affirmatively, rather than based on a pre-selected confirmation. As noted under Recital 32 of the GDPR, ‘this could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which clearly indicates in this context that the data subject’s acceptance of the

⁴⁰ Koops above n7 at 251.

⁴¹ EDPB 2020, Para 41.

⁴² Ibid p.15.

proposed processing of his or her personal data'. Silence, pre-ticked boxes, or inactivity on the part of the data subject does not constitute consent.⁴³

In summary, when a user provides consent for the processing of personal data by a digital platform, it can only be valid if the digital platform can demonstrate that the consent was freely given, the data subject was informed, consent was for a specific purpose, and the agreement to the processing of data was unambiguous.⁴⁴ The next section analyzes in detail the conditions under which a digital platform's data processing terms of use, as they relate to the obtaining of consent, could lead to anti-competitive conduct, thereby invoking the jurisdiction of competition agencies.

3.0 Is a Lack of Valid Consent to Processing of Personal Data by Digital a Competition Law Concern?

This paper argues that a digital platform's data processing terms of use become a competition law concern because: data is a source of market dominance; the data processing terms of use constitute an anti-competitive conduct; the legal test of the anti-competitive conduct is met; the conduct leads to a competition harm; and the causality requirement under competition law linking the anti-competitive conduct to harm is met.

3.1 Data as a source of market dominance

In competition law, a firm holding a dominant position is not inherently illegal. What is illegal is when a firm abuses its dominant position by engaging in exclusionary or exploitative conduct, such as price fixing, market allocation, predatory pricing, and unfair trading conditions. Thus, the general rule is that a firm's dominant position is a necessary but not sufficient condition to prove an abuse.⁴⁵ For a long time, a firm's dominance has been measured by its market share in terms of price. However, it is now widely accepted that there are different non-price metrics for measuring a firm's market dominance, and data is one of them.⁴⁶

According to Paal, access to data entrenches a digital platform's market dominance.⁴⁷ Unlike traditional businesses, which have access to data on their own users, digital platforms

⁴³ EU GDPR, Recital 32.

⁴⁴ See Article 7 of the GDPR which provides for conditions for consent.

⁴⁵ Nora von Ingersleben-Seip and Zlatina Georgieva, 'Old Tool for the New Economy? Counterfactual Causation in Foreclosure Assessment and Choice of Remedies on Data-Driven Markets' (2025)13 *Journal of Antitrust Enforcement* 328, 343.

⁴⁶ Knapstad above n 18; Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 (4) *World Competition* 473.

⁴⁷ Boris P Paal, 'Market Power in Data (Protection) Law' (2021) 2(1) *Global Privacy Law Review* 8.

can access vast amounts of data from their users and from third parties. By harnessing and processing extensive data, digital platforms can accurately create and improve existing personalized products and services while also engaging in targeted advertising aligned with consumer preferences and recommendations, granting them a competitive advantage over their rivals. As observed by Rubinfeld and Gal, ‘those who enjoy more portholes from which to gather data, who have a substantial database to which they can compare new data, or who possess unique data synthesis and analysis tools, may enjoy a competitive advantage’.⁴⁸

If data is a non-price metric of market dominance, a crucial starting point for competition agencies is therefore understanding that access to vast amounts of data through data processing terms of use grants digital platforms significant data power. Majcher defines data power as a subcategory of market power that is ‘concerned with power that results from access to personal data as well as other structural features that data enables, such as the creation of digital ecosystems’.⁴⁹ Data power stems, in large part, from a digital platform’s ability to access, process, and control data.

The data power consequently enables digital platforms to gain and leverage other forms of power identified in the competition law literature, such as market power, digital ecosystem power, and gatekeeping power,⁵⁰ thereby strengthening their dominant positions. For example, in competition law, market power is defined as ‘the ability of a company or a group of companies to establish their policies, such as their prices, product quality, and investments in innovation, to a significant extent without a severe competitive constraint from competitors, customers, or consumers’.⁵¹ Data power can increase the digital platform’s market power, resulting in what Stucke refers to as data oligopolies.⁵² Data power also enhances a digital platform’s ecosystem power, which refers to the ability to enter and leverage adjacent markets, thereby creating a digital ecosystem with interconnected services.⁵³ Consequently, it is not surprising that, in the quest for digital ecosystem power, digital platforms are likely to engage in privacy policy tying and bundling, enabling them to combine user data through bundled

⁴⁸ Daniel L Rubinfeld and Michal S Gal, ‘Access Barriers to Data’ (2017) 59 Arizona Law Review 339, 342.

⁴⁹ Majcher above n13 at 158.

⁵⁰ Gatekeeping power refers to the ability of a digital platform to control access to its services in a structured manner when it acts as an intermediary between end-users and business users.

⁵¹ Adriana Hernandez Perey and Aldo Gonzalez, ‘Market Power’ (Concurrences Competition Law Dictionary, Art, No 12330), 1.

⁵² Maurice E Stucke, ‘Should we Be Concerned about Data Opolies’ (2018) 2 GEO. L. TECH Review 275.

⁵³ Daniele Condorelli and Jorge Padilla, ‘Data-Driven Envelopment with Privacy-Policy Tying’ (2024) 134(658) The Economic Journal 515.

consent.⁵⁴ Combining data across integrated platforms enables digital platforms to enter related and unrelated markets, build ecosystems, lock in consumers, and potentially foreclose rivals.

Given the role of data in the success of tech companies' business models, competition for data among digital platforms has altered the competitive landscape. In van de Waerdt's view, 'there is no longer competition on the market, nor even for the market: it is competition for *data*'.⁵⁵ This analysis leads to the expectation that a digital platform's data processing terms of use may become a competition law concern because they enable the platform to collect data, strengthen its market dominance, and likely create opportunities for digital platforms to abuse this power, as prohibited under competition law.

3.2 Data processing terms of use as a competition law violation

Competition agencies must demonstrate that the digital platform's data-processing terms of use constitute a competition law violation, thereby providing them with the legal basis to investigate the conduct. In competition law, anti-competitive conduct can be either exclusionary or exploitative. Unlike exclusionary conduct, where a dominant firm seeks to exclude rivals from the market, exploitative abuses are 'unilateral behaviours by dominant firms that distort competition in the market by directly harming consumers, rather than excluding competitors'.⁵⁶ Let's examine how digital platforms can utilize data to engage in exclusionary or exploitative behavior.

a. Exclusionary conduct

Concerning exclusionary conduct, competition agencies are increasingly paying attention to how tech companies use mergers and acquisitions to combine and accumulate data and later engage in exclusionary conduct, excluding rivals from access to data. For example, during the 2014 *Facebook/WhatsApp* acquisition, while critics of the merger argued that Facebook would change WhatsApp's Privacy policy post-merger to access WhatsApp user data,⁵⁷ the EU Commission (EC) approved the merger.⁵⁸ The EC recognized that Facebook's position would be entrenched if WhatsApp were the sole source of user data for Facebook, which, in its view, was not the case.⁵⁹ At that time, the EU Commission held that, unlike Facebook, WhatsApp

⁵⁴ Ibid.

⁵⁵ Peter J. van de Waerdt, 'From Monocle to Spectacles: Competition for Data and "Data Ecosystem Building"', (2023) 19(2) *European Competition Journal* 191, 196.

⁵⁶ Marco Botta and Klaus Wiedemann, 'Exploitative Conducts in Digital Markets: Time for Discussion After the Facebook Decision' (2019) 10(8) *Journal of European Competition Law & Practice* 465, 465.

⁵⁷ Vicente Bagnoli, 'Questions that Have Arisen since the EU Decision on the WhatsApp Acquisition by Facebook' (2019) 3(1) *Market and Competition Law Review* 15.

⁵⁸ Facebook/WhatsApp (Case COMP.M.7217) Commission Decision [2014] OJ C417/02

⁵⁹ Ibid paras 180-183.

was not involved in the online advertising market, nor did WhatsApp collect extensive user data like Facebook. In its view, in the presence of alternative online advertising platforms such as Google, the EC held that the merger did not negatively affect competition. The EC also noted that a data protection violation was not a concern of a competition agency and explicitly stated that, ‘any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law but within the scope of the EU data protection rules’.⁶⁰

What the EC did not anticipate, and did not consider a significant issue, was the possibility that Facebook would alter WhatsApp’s privacy policy after the merger to access WhatsApp’s data set. In August 2016, WhatsApp announced a change to its data policy that would link users’ phone numbers to their Facebook identities and require WhatsApp users to accept the combination of WhatsApp data with Facebook to use WhatsApp.⁶¹ In 2017, following a formal investigation, the EC fined Facebook €110 million for providing misleading information. Evidently, Facebook’s acquisition of WhatsApp in 2014 was primarily a strategy to access extensive user data for its advertising model and to enhance its data capabilities. Thus, tech companies understand the role of data in increasing their market dominance. Thus, competition agencies need to monitor the said digital platforms and investigate their capability to engage in exclusionary conduct, such as limiting data portability and access.

b. Exploitative abuse

One way to infer whether a digital platform’s data processing terms can lead to exploitative abuse is to examine the power imbalances between the digital platform and the users. Generally, digital platforms have become essential for users to access products and services. E-commerce platforms, for instance, have enabled users to purchase products at their convenience. Because users derive benefits from digital platforms, this creates a stronger incentive to consent to the processing of their personal data, with a reasonable expectation that the more a platform has access to their personal data, the more personalized their experience will be.

Notably, the more data a digital platform has, the greater its data network effects become, increasing its value to users. Ingersleben-Siep argues that ‘data network effects occur when the collection of an additional data point makes a product or a service more valuable to

⁶⁰ Ibid, para 164.

⁶¹ Maria Paz Canales and Michel Roberto de Souza, ‘What’s UP, Latin America? Between Competition, Data and Consumer Protection’ (2022) 71(10) GRUR International 967.

its users’.⁶² Like network effects,⁶³ data network effects can lock in consumers on a particular platform. Unfortunately, even when alternatives exist, users may be inclined to provide their personal data to multiple platforms offering the same products and remain locked to one platform with which they are willing to share data.

To increasingly benefit from data network effects, digital platforms are also using unscrupulous, invasive, and intrusive data collection and processing tools to access and control data, such as data mining and surveillance, through their data processing terms of use, regardless of whether users accept them.⁶⁴ Digital platforms’ data collection strategies are enabled by mergers and acquisitions, extensive data extraction, third-party tracking, and, recently, the integration of artificial intelligence (AI) tools into their core services. AI tools such as Microsoft Copilot, Meta AI, and Google Gemini enhance tech companies’ ability to analyze data with high precision and adopt new products and services. This analysis has also enabled companies to analyze their competitors and develop strategies that reduce competition and increase profits, while at the same time infringing data protection law.⁶⁵

Strictly speaking, the power imbalances between digital platforms and users diminish users’ bargaining power and choice, allowing digital platforms to impose unfair conditions in the processing of personal data. As Balasingham and D’Amico put it, ‘the customers have no choice but to accept unfair terms or excessive prices’.⁶⁶ What makes it even worse, as noted by Li, ‘since there is a lack of transparency regarding the excessive collection and (mis)use of data, misleading information, and behavioural manipulation, consumers seem to be overwhelmed and unable to make rational, well-informed decisions concerning their personal data’.⁶⁷ That is why, when power imbalances exist, the GDPR raises questions about whether consent can serve as a lawful justification for data processing. Recital 43 of the GDPR provides that:

⁶² Nora von Ingersleben-Siep, ‘What are Data Network Effects and What is their Impact on Market Competition?’ (Medium, 5 Feb 2020).

⁶³ Network effects –direct or indirect– increase digital platforms’ data power. And because of the lock in effects, it enables the digital platform to excessively and aggressively collect data from its end-users, irrespective of consent.

⁶⁴ Katharine Kemp, ‘Concealed Data Practices and Competition Law: Why Privacy Matters’ (2020) 16 (2-3) *European Competition Journal* 628.

⁶⁵ Boris P Paal, ‘Artificial Intelligence as a Challenge for Data Protection Law’ in Silja Voenekey, Philipp Kellmeyer, Oliver Mueller and Wolfram Burgard (eds), *The Cambridge Handbook of Responsible Artificial Intelligence* (Cambridge University Press 2022) 290-308.

⁶⁶ Baskaran Balasingham and Alessia S D’Amico, ‘Beyond Exclusion: Revisiting Exploitative Abuses in Digital Platform Markets’ (2025) 13 *Journal of Antitrust Enforcement* 265, 266.

⁶⁷ Qian Li, ‘Excessive Data Collection and (Mis)use of Data: A Comparative Law and Economics Study on the Chinese Didi Case and the German Facebook Case’ (2025) 13 *The Chinese Journal of Comparative Law* 1, 3.

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case *where there is a clear imbalance between the data subject and the controller*, in particular where the controller is a public authority and it therefore unlikely that consent was freely given in all the circumstances of that specific situation’ (Emphasis added).

Under the GDPR, where a clear imbalance of power exists, consent can only be used as a valid reason for processing data in exceptional circumstances.⁶⁸ This could happen when the data controller, in tandem with the accountability principle, demonstrates that there will be no adverse consequences for the data subject if they do not consent. And secondly, when the data subjects are offered an alternative that will not have any negative impact on them. In assessing the power imbalances, competition agencies should consider the ‘position of the large online platform in the market, the existence of lock-in or network effects, the extent to which the data subject relies on the service, and the main audience of the service’.⁶⁹

Competition agencies, therefore, can infer power imbalances between the digital platform and the user to assess the likelihood that the data processing terms of use will violate competition law through exploitative abuse. Since the Bundeskartellamt-Facebook decision, which identified Facebook’s conduct as exploitative, commentators argue that exploitative abuse in digital markets, where personal data is the price users pay to access zero-priced services, occurs through excessive data collection and unfair trading conditions. If so, analysis of the legal test for demonstrating a digital platform has engaged in excessive data collection and unfair trading conditions is critical.

3.3 Assessing the legal test of exploitative conduct under competition law

According to emerging literature, the terms of use for data processing on a digital platform can constitute exploitative practices, such as excessive data collection or unfair trading conditions.⁷⁰

a. Lack of valid consent in the processing of personal data by digital platforms, as excessive data collection

Competition policy scholars have noted that data processing terms that require combining data from other sources with the digital platform’s data, and where such data is not necessary for the provision of the specific service for which consumers provide personal data, constitute

⁶⁸ EDPB 2023, para 12

⁶⁹ EDPB, 2024 at 3.

⁷⁰ Balasingham and D’Amico above n66; Kerber and Zolna above n37.

excessive data collection, akin to excessive pricing under competition law.⁷¹ Although excessive data collection is often compared to excessive pricing, the legal test for excessive pricing in competition law is contentious, as are the approaches of competition agencies.⁷² In the EU, for example, the legal test for determining excessive pricing was set out by the CJEU in the *United Brands* case.⁷³ In determining whether the prices charged by *United Brands* to banana distributors in the EU were *excessive*, the CJEU held that a price is excessive if the difference between the cost of production and the price charged lacks a reasonable relationship to the product's economic value. Secondly, the prices should be considered *unfair* if it can be shown that the dominant undertaking took advantage of its position to reap profits that it could not have achieved in the absence of normal and sufficiently effective competition.⁷⁴

If the excessive pricing legal test set out by the CJEU in *United Brands* were to be applied to cases involving excessive data in digital markets, it would, unfortunately, face both conceptual and practical challenges. Competition agencies, for instance, will face a challenge in determining whether they can equate data to price. Although some economists have argued that monetary value can be attached to personal data,⁷⁵ in most cases, data has non-monetary value, such as privacy protection, making it difficult to quantify its value in monetary terms. Moreover, unlike price, users can share their data with multiple digital platforms at different times. As illustrated by Haucap, that:

It is conceptually much more difficult to construct an exploitative abuse case, as users are not left with less data than they had before. This is a fundamental difference to excessive pricing cases where customers are left with less money/wealth once they have been exploited.⁷⁶

In addition to quantifying data as price, assessing data excessiveness also presents evidentiary challenges, particularly when determining the volume of personal data collected by a digital platform through both first-party and third-party tracking. Moreover, limiting the data a platform collects can affect product quality, as firms need more data to analyze and improve their products. Thus, one might even question at what point a competition agency can determine

⁷¹ Anne C Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021) 66(2) *The Antitrust Bulletin* 276; Viktoria Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57(1) *Common Market Law Review* 161.

⁷² Ryan David McKerrow, 'Excessive Pricing in South African Competition Law: Elucidating the Nature and Implications of the Consumer-Detriment Requirement' (2017) 29(2) *SA Mercantile Law Journal* 1

⁷³ Case 27/76 *United Brands v Commission*, ECLI:EU:C:1978.

⁷⁴ Witt above n71, at 278.

⁷⁵ On attaching monetary value to data see, Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34(2) *Computer Law & Security Review* 289.

⁷⁶ Justus Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German *Facebook* Decision' (2019) *CPI Antitrust Chronicle* 1, 3.

that legitimate data collection has ended and excessive data collection has begun. Furthermore, unlike in cases of excessive pricing, where excess prices can be evaluated by comparing the product's cost and production costs, establishing production costs in digital markets can be challenging due to the economies of scale that characterize online markets. In excessive pricing, it is easy to compare prices across similar relevant markets to determine unfairness. In digital markets, however, research has shown that digital platforms typically have the same privacy policies or terms regarding user data, making it challenging to find comparable services.⁷⁷

Despite the challenges of conceptualizing excessive data collection, there is still some hope. Some scholars have argued that competition agencies can determine whether a digital platform is engaging in excessive data collection in absolute or relative terms by considering whether the data collected is used beyond what is necessary to provide the specific service to which users expect their personal data to be used for.⁷⁸ This observation aligns with the principle of data minimization in data protection law, which requires that when processing personal data, the data should be adequate, relevant, and limited to what is necessary in relation to the purpose for which it was collected.⁷⁹ In other words, the purposes for collecting personal data should be sufficiently distinct and legitimate, reflecting the element of consent as specific. Thus, when digital platforms collect data through third-party tracking tools and data brokers, which gather extensive information from various sources and use it for purposes to which users did not consent, this can be deemed excessive data collection.⁸⁰ This analysis suggests that data collection is likely to be deemed “excessive” by a competition agency if a digital platform uses data collected from a user for a purpose other than that for which the user originally consented.

b. Lack of valid consent as unfair trading conditions

In determining unfair trading conditions as noted by Botta and Wiedemann, ‘not the quantity of data collected is under scrutiny, but the question of how data is processed, who gets access, and how transparent the “data for services” deal is’.⁸¹ Thus, unlike excessive data collection, unfair trading conditions in competition law assessments constitute obligations imposed by a dominant firm that are not absolutely necessary or proportionate for the attainment of a

⁷⁷ Ariel Ezrachi and Viktoria Robertson, ‘Competition, Market Power and Third-Party Tracking’ (2019) 41(1) *World Competition* 15.

⁷⁸ Robertson above n71.

⁷⁹ See, for example, Article 5(1, c) of EU GDPR.

⁸⁰ EDPB Opinion 08/2024. Para 140.

⁸¹ Botta and Wiedemann above n 55 at 469.

legitimate objective and directly harm users by restricting their freedom in an erroneous manner.⁸²

Power imbalances between the digital platform and users can exacerbate the platform's ability to impose unfair trading conditions on users through unreasonable terms of use. By focusing on unfair trading conditions, a competition agency can assess exploitative conduct qualitatively by closely monitoring a digital platform's terms of use, as reflected in its user data and privacy policies. However, what constitutes an unfair trading condition is a complex factor that must be determined on a case-by-case basis by a competition agency. For instance, as scholarly work on data protection and competition law reveals, when users consent to the combination of their personal data from third parties with a digital platform's core platform service, which is conditioned on access to and use of the digital platform, and such data combination is not necessary for the provision of the digital service, these particular terms of service could constitute unfair trading conditions.

3.4 Developing a theory of harm

It has been argued that if competition agencies treat data breaches as a competition law concern, they will grapple with how to develop a competition harm by incorporating privacy harms into competition assessments. The argument is that any harm identified by the competition agency relating to data collection terms of use by digital platforms must be a realistic harm to competition in the form of impeding the competitive process or hindering effective competition. Some policymakers argue that privacy harm can be evaluated as a non-price dimension of competition in zero-priced digital markets.⁸³ Privacy harm is then conceptualized as degraded product quality or limited consumer choice, which are concerns for competition law because they result in market failure in digital markets.⁸⁴

a. Degraded product quality

In digital markets where products or services are offered for free, product quality has become the primary competitive dimension and bargaining chip upon which digital platforms procure user consent. Unfortunately, as argued by Stucke and Ezrachi, in multisided markets where a firm earns profit from one side, it may degrade quality on the other side through invasive data

⁸² Pinar Akman, 'The Role of Exploitation in Abuse under Article 82 EC' (2009) 11 Cambridge Yearbook of European Legal Studies 11.

⁸³ Esayas above n12.

⁸⁴ Samson Y Esayas, 'Competition in (data) Privacy: "zero"-Price Markets, Market Power, and the Role of Competition Law' (2018) 8(3) International Data Privacy law 181.

collection if doing so increases its profitability on the first side.⁸⁵ According to Gorecka, ‘if reduction of a product’s quality is actionable under competition law and consumers see privacy as an aspect of quality, then reduction of privacy could arguably be seen as a consumer harm in any competition assessment’.⁸⁶ If product quality degradation can be considered a parameter of competition, then competition agencies could infer that competition harm is likely to occur when the quality of the digital platform’s service is degraded, unless users consent to the digital platform’s data processing terms of use.

b. Limited choice

Some scholars argue that the lack of valid consent for the processing of personal data on digital platforms limits consumer choice, constituting a significant harm to competition due to the lack of effective competition.⁸⁷ Moreover, in the absence of viable alternatives and where data collection terms of use are premised on a take-it-or-leave-it basis, users have no or limited choice but to provide their personal data, even when the data collection and processing exceed their reasonable expectations. Thus, competition agencies can infer that a competition harm in the form of limited choice is likely to occur when users’ access and use of digital platforms is conditioned on the user’s consent to the digital platform’s personal data processing terms of use, which the user would not consent to if effective competition existed.

3.5 The causation requirement

If the lack of valid consent in the processing of data by digital platforms is deemed to result in exploitative conduct, in most jurisdictions, strict causation (conduct causality) is required to establish the necessary factual link between the anti-competitive conduct and the resulting market harm.⁸⁸ In this case, a competition agency must demonstrate that, had the exploitative conduct not occurred, the harm would not have occurred.⁸⁹ Because conduct causality tends to be more stringent, competition agencies have intervened only to investigate exploitative abuses in exceptional circumstances. Thus, how competition agencies will address the causality requirement will vary from one country to another, depending on their case law and the provisions of their specific legislation. This paper interrogates how the German

⁸⁵ Maurice E Stucke and Ariel Ezrachi, ‘When Competition Fails to Optimize Quality: A Look at Search Engines’ (2016) 18 *Yale Journal of Law & Technology* 70. 72.

⁸⁶ Gorecka above n14 at 560.

⁸⁷ Rachel Scheele, ‘Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice’ (2021) 12 (1) *Journal of European Competition Law & Practice* 34.

⁸⁸ von Ingersleben-Seip and Georgieva above n44.

⁸⁹ See Gregory J Werden, ‘Exploitative Abuse of Dominant Position: A Bad Idea that now Should be Abandoned’ (2021) 17(3) *European Competition Journal* 682.

Bundeskartellamt, the OLG, the FCJ, and the CJEU addressed the causality requirement in the Bundeskartellamt/Facebook decision.

4.0 Reassessing the 2019 Bundeskartellamt/Facebook Decision

The Bundeskartellamt/Facebook case is divided into four subsections: the 6 February 2019 Bundeskartellamt decision; the 26 August 2019 OLG decision; the 23 June 2020 FCJ decision; and the 4 July 2023 CJEU decision.

4.1 The 2019 Bundeskartellamt decision against Facebook

a. Assessing market dominance

In its view, and in accordance with the argument of this paper that data is a source of tech companies' dominance, the Bundeskartellamt submitted that, in multi-sided markets where services are zero-priced for users, the specific characteristics of such markets must be considered when determining market dominance.⁹⁰ Thus, from paragraphs 374 to 521 of its decision, the Bundeskartellamt emphasized that Facebook's multiple data sources, along with network effects, lock-in effects, and high user switching costs, entrenched its dominance.

In determining Facebook's market dominance, the Bundeskartellamt first analyzed Facebook's market share in the German social networking market. Recognizing the impact of network effects and user lock-in, the Bundeskartellamt employed a user-based indicator to determine how the number of active monthly users in Germany can entrench a digital platform's dominance.⁹¹ It found that Facebook's user base market share in the relevant social network market was above 80% for monthly active users and above 50% for registered users in Germany. Facebook held a dominant position in the German social network market, based on its market share and user base.

b. Identifying the anti-competitive conduct

The Bundeskartellamt found that Facebook had abused its dominant position by engaging in exploitative conduct, specifically unfair business practices, pursuant to the general clause of Section 19(1) GWB through its terms of use. The Bundeskartellamt identified Facebook's data processing terms as terms within the meaning of Section 19(1) and (2) no.2 GWB.⁹² In tandem with this paper's argument, the Bundeskartellamt therefore began its analysis by demonstrating

⁹⁰ Bundeskartellamt, Case B6-22/16, Para 386-387.

⁹¹ Ibid para 405-413.

⁹² Ibid para 524.

the legal basis for investigating Facebook's conduct under the abuse of dominant position provision of the GWB.

c. Assessing the legal test of the exploitative conduct by Facebook

The Bundeskartellamt argued that Facebook had engaged in unfair trading terms and excessive data collection contrary to the GWB. As discussed earlier, although data can be considered a non-price dimension of competition, demonstrating the legal test for excessive data collection is complex, especially in determining when the data is "excessive". Despite Facebook's argument that combining data was necessary to provide users with services that reflect their personal preferences across its platforms, the Bundeskartellamt submitted that the additional off-Facebook data that Facebook sought to combine with its social network was not necessary for the provision of its social networking services. The reason was that there was no contractual link between Facebook and other Facebook-owned services (Instagram and WhatsApp), including Facebook Business Tools, which required independent registration and separate user contracts.⁹³ In accordance with the expectations of this paper, the Bundeskartellamt measured the 'excessiveness' of Facebook's data collection strategies in absolute terms by focusing on whether the additional data collected by Facebook was necessary for the provision of the social networking service, which the users had ascribed to when sharing data.

The Bundeskartellamt also ruled that Facebook's terms of use, which required users to consent to the collection of extensive data from third-party websites and other Facebook-owned services, as detailed in its data and cookie directive on conditional use of Facebook, constituted unfair trading terms.⁹⁴ In determining the unfairness of Facebook's data processing terms of use, the Bundeskartellamt questioned whether the conditionality of consent obtained by Facebook was a fair business term. In the Bundeskartellamt's reasoning, the Facebook terms of consent constituted unfair trading terms because 'agreeing to the Terms of Service, which users are required to do in order to be able to use the social network, does not constitute voluntary consent pursuant to Article 6(2a) of GDPR'.⁹⁵ In particular, Facebook did not obtain users' consent during the registration process for their profiles. Rather, it relied on users agreeing to the Terms of Service by clicking the 'register' button. Consent was only mentioned as a legal basis for collecting data in its terms of use. Again, as discussed earlier, it is for the

⁹³ Ibid para 680.

⁹⁴ Ibid paras 535-558.

⁹⁵ Ibid para 641.

competition agency to determine, on a case-by-case basis, when data processing terms of use are unfair.

d. Theorizing competition harm

If Facebook users had suffered a privacy harm, the Bundeskartellamt, in developing the theory of harm in competition terms, had to show how Facebook's data processing terms led to a competition harm. Facebook had contested that the Bundeskartellamt could not provide an economic quantification of harm because its users did not pay for using the social network.⁹⁶ In response, the Bundeskartellamt argued that harm can be assessed in non-monetary terms because, in addition to excessive prices, 'unconstrained scope of action can also lead to diminished product volume and less quality, less variety as well as less dynamic innovation'.⁹⁷ In particular, the Bundeskartellamt pointed out that 'the scope for setting prices is not the only relevant factor in defining market power'.⁹⁸ Therefore, in markets where services are offered free of charge, 'in economic terms, the price of zero must also be considered to be a price'.⁹⁹ The Bundeskartellamt also recognized the difficulty of quantifying harm as it relates to privacy and held that:

It is difficult to quantify the effects of the damage, since it is not clear whether, when, and how potential material or, in particular, immaterial consumer damage will occur, and which users will be affected. It is not possible to predict either what damage potential the data may have as a result of possibilities for combination or technical analysis that may not be available currently, but could well be in the future.¹⁰⁰

Nonetheless, the Bundeskartellamt argued that Facebook users suffered privacy harm in the form of diminished quality. According to the Bundeskartellamt, the potential for damage increased 'with the scope and quality of the data, Facebook data from Facebook-owned services or Facebook Business Tools allows conclusions to be drawn about the history of sensitive websites accessed by users,' leading to privacy harm.¹⁰¹ The Bundeskartellamt also noted that German users faced limited choice, a concern under competition law. Actually, as the Bundeskartellamt illustrated, due to the conditionality of access, users had no genuine choice, and withdrawal of consent was detrimental because Facebook provided German users with a take-it-or-leave-it option, in contravention of Article 4(11) of the GDPR. This observation aligns with Article 7(4) of the GDPR, which stipulates that conditional access to a

⁹⁶ Ibid para 906.

⁹⁷ Ibid Para 377

⁹⁸ Ibid para 377.

⁹⁹ Ibid para 378

¹⁰⁰ Ibid para 912

¹⁰¹ Ibid para 910.

service with no contractual link should be taken into account when determining whether consent was freely given.¹⁰² Additionally, even if clicking ‘I agree’ constitutes users’ willful consent to data processing, the consent could not be deemed voluntary because it was affected by power imbalances between Facebook and its users, which reduced the user’s bargaining power to make a choice. The Bundeskartellamt also noted that German users were locked into Facebook due to strong direct and indirect network effects, limiting their ability to switch to alternatives.¹⁰³ In summary, by incorporating privacy harm into competition assessment, the Bundeskartellamt treated it as a non-price dimension of competition harm, manifested in degraded product quality and limited user choice. Harms that are competition harms.

e. Determining the causality requirement

In exploitative conduct cases, most competition agencies take the approach that strict causality, in the form of conduct causality, is required, showing that the firm’s anticompetitive conduct caused the competition harm. Regarding the causation requirement, although the Bundeskartellamt identified Facebook’s conduct as exploitative, it acknowledged that conduct causality was not required. For the Bundeskartellamt, result causality (also known as normative causality), which holds that harm to competition is guided by the results or outcome rather than merely by the conduct itself, was required. In the result causality, what was required was to demonstrate that the dominant position amplified the anti-competitive effects of the digital platform’s exploitative behavior. Specifically, the Bundeskartellamt held that:

For the “abuse” of a dominant market position, according to general rules, it is sufficient for there to be “normative causality” between market dominance and the conduct. It is sufficient if the conduct proves to be anticompetitive as a result of market dominance, which does not require strict causality but rather a causality in relation to the outcome.¹⁰⁴

According to the Bundeskartellamt’s interpretation, Facebook’s market power enabled it to collect excessive data and force users to accept its terms of use, which allowed it to combine additional data from other sources, even though this was not necessary for the use of the social network for which they had registered. Furthermore, due to its market power and lack of transparency in data processing, Facebook was able to process data even against the will of users who had ‘no choice but to consent to their data being processed’.¹⁰⁵ Were it not for its dominant position, and in a market with effective competition, Facebook would be

¹⁰² Ibid, para 645.

¹⁰³ Ibid, paras 423-476.

¹⁰⁴ Ibid, para 873.

¹⁰⁵ Ibid para 385.

incentivized to offer better and user-friendly terms of use. Thus, according to Bundeskartellamt, the result causality was sufficient to establish a link between Facebook's dominant position and the exploitative abuse.¹⁰⁶

f. Analysis

The Bundeskartellamt decision was met with applause and contempt. Critics argued that by relying on result causality, the Bundeskartellamt failed to develop a clear theory of harm. It failed to show how Facebook's conduct (exploitative abuse) had harmed consumers, as required under conduct causation. Others argued that by examining whether Facebook's data policy complied with the GDPR, the Bundeskartellamt extended its jurisdiction into data protection law. According to Colangelo, the Bundeskartellamt:

Acted as a self-appointed enforcer of data protection rules, finding the existence of a privacy violation previously undetected by any data protection authority, and interpreting data protection rules in a restrictive way that goes far beyond the limits of its legal competence. Further by placing a special privacy responsibility on dominant firms, the FCO's approach is rooted in the idea that virtually every legal infringement by a dominant firm could amount to an antitrust violation.¹⁰⁷

Facebook, aggrieved by the decision, appealed to the Oberlandesgericht Düsseldorf (German Higher Regional Court, OLG) on February 11, 2019. It was expected that the OLG would address the issues raised by critics, especially those concerning the theory of harm and the causation requirement.

4.2 The Düsseldorf Oberlandesgericht decision

On 26 August 2019, the OLG suspended the Bundeskartellamt's decision in favour of Facebook, expressing serious doubts about its legal basis.¹⁰⁸ The OLG had issues with how the Bundeskartellamt assessed the anti-competitive conduct, developed the theory of harm, and met the causation requirement in the context of exploitative conduct.

a. Assessing the anti-competitive conduct

The OLG noted that the Bundeskartellamt had failed to prove that Facebook had indeed engaged in excessive data collection by demonstrating the 'excessiveness' of the data. To the OLG, users' participation in Facebook's social networking service depended on data

¹⁰⁶ Alba Ribera Martinez, 'The Court of Justice Kicks Around the Dichotomy between Data Protection and Competition Law: Case Comment of the Preliminary Ruling in Case C-252/21 Meta Platforms v. Bundeskartellamt' (2023) 28 Yearbook of Antitrust and Regulatory Studies 131,139.

¹⁰⁷ Giuseppe Colangelo, 'Facebook and Bundeskartellamt's Winter of Discontent' (Competition Policy International 2019) 4.

¹⁰⁸ Higher Regional Court of Dusseldorf, decisions of 26 August 2019, Case VI-Kart 1/19 (V) (OLG Decision) Available at <https://www.d-kart.de/wp-content/uploads/2019/08/OLG-Düsseldorf-Facebook-2019-English.pdf> accessed 12 December 2024.

processing, and Facebook's access to additional data was to be balanced against the use of an advertising-financed social network and the user's benefits of a personalized experience when Facebook accessed additional data. Furthermore, 'not every excess of what is still permissible according to competitive standards leads to the assumption of abuse of market power'.¹⁰⁹ Thus, according to the OLG, the Bundeskartellamt had failed to provide any meaningful findings regarding the type, origin, and quantity of the additional data in question. In doing so, the Bundeskartellamt failed to provide evidence that the additional data, which Facebook combined from third-party sources, constituted an excess. This observation clearly shows the challenge competition agencies will face in determining the excessiveness of data.

Additionally, the OLG noted that, for the test of excessiveness to be sufficient, the Bundeskartellamt had to demonstrate a considerable gap between the terms and conditions demanded and those in conformity with the principles of competition. This was to be assessed against the collection of user and device data from the company's other services, such as WhatsApp, Instagram, Oculus, and Masquerade, as well as from other Facebook Business Tools. Then determine the anti-competitiveness of these additional data, combined with Facebook. The Bundeskartellamt, therefore, failed to conduct sufficient investigations into the 'as-if-competition' test by considering the conduct of other undertakings in comparable markets. This observation reflects the challenge of determining the unfairness of excessive data collection in a market with limited comparables.

b. Theory of harm

The OLG rejected the Bundeskartellamt's theory of harm, that users had suffered a privacy harm as a result of Facebook's dominant position. In the OLG's view, there was no evidence that users had suffered a financial loss.¹¹⁰ This is despite the Bundeskartellamt putting forward the argument that 'users might potentially suffer material (financial) harm if Facebook discloses data to third parties, whether intentionally or unintentionally, for instance, leading to identity theft, extortion or fraud'.¹¹¹ Moreover, the OLG submitted that, unlike an unpaid fee, data can be duplicated by other digital platforms. Thus, German Facebook users were at liberty to make their 'data available to any third party, including Facebook competitors on the social networking market, as often as they like'.¹¹² This observation by the OLG sheds light on the

¹⁰⁹ OLG Decision, English version, at 8.

¹¹⁰ Klaus Wiedemann, 'A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)' (2020) 51 IIC 1168, 1170.

¹¹¹ Case B6-22-16, para 910.

¹¹² OLG Decision, English Version, at 7-8.

debate over whether a privacy harm can be considered a non-price dimension of competition harm.

In refuting the claim that German users had suffered harm in the form of limited choice, the OLG noted that there was no loss of user control or of the right to self-determination, as asserted by the Bundeskartellamt.¹¹³ The reason is that there was no evidence that Facebook obtained users' consent through coercion, pressure, exploitation of a weakness of will, or any other unfair means. To the OLG, German Facebook users gave their consent willingly and made a conscious decision, based on rational calculation, to take advantage of Facebook's benefits. According to Colangelo, the OLG thought that 'users can undertake such balancing without being unduly influenced, and do so completely autonomously, according to their own preferences and values'.¹¹⁴ Indeed, to emphasize that German Facebook users had a choice, the OLG noted that only 32 million German users used Facebook monthly, compared to 50 million Germans who were non-Facebook users, which provided evidence that German users had *a choice* about whether to use Facebook. Regarding the user's choice, it appears that the OLG overlooked the consequences of power imbalances between a dominant digital platform and users, which can undermine users' ability to make an informed choice regarding the processing of personal data.

The OLG further argued that the Bundeskartellamt had focused on a data protection issue rather than a competition problem. Yet users' harm in itself should not be based on a GDPR violation but on a theory of harm under competition law. Furthermore, the Bundeskartellamt failed to demonstrate that Facebook's exploitation of users, resulting from the conditions on the collection and combination of data, which is detrimental to competition, was caused by the data protection law. In summary, the OLG's reasoning on the theory of harm requires the competition agency to demonstrate how the specific harm constitutes a competition harm. If limited choice is treated as a harm to competition, then competition agencies should demonstrate how the loss of user control manifests in the alleged anti-competitive conduct.

c. The causation requirement

The OLG further contended that even if German users suffered harm, the Bundeskartellamt had failed to establish the necessary strict causal link between Facebook's alleged exploitative conduct and the harm suffered by those users. If causality is to be confirmed, the OLG argued that the anti-competitive effects of the abusive conduct must also be confirmed by

¹¹³ OLG Decision, English version at 9.

¹¹⁴ Colangelo above n107, at 3.

demonstrating that the alleged conduct was the direct cause of the harm (conduct causality), rather than by reasoning that the conduct had a negative result (result causality).¹¹⁵ In other words, causality exists if it can be demonstrated that, had the firm not acted, the users would not have suffered harm.¹¹⁶

Consequently, the OLG held that the Bundeskartellamt did not adequately demonstrate that Facebook's combination of additional data from third-party sources was a direct cause of the user's harm, namely, limited choice. The Bundeskartellamt focused on demonstrating the causal link between dominance and exploitation, which, in the OLG's view, was insufficient. In Facebook's case, the OLG argued that there was 'no causal connection between the illegitimate data processing and the firm's market power'.¹¹⁷ The conduct of a dominant firm can only be considered abusive exploitation of consumers when the agreed-upon conditions are disadvantageous to the consumer due to their content, rather than because of the firm's dominance.¹¹⁸ Thus, in the OLG's reasoning, the Bundeskartellamt was required to prove conduct causality and not result causality.

d. Analysis

In summary, the OLG decision clearly demonstrates that competition agencies must go beyond merely showing that there is an exploitative abuse, evidenced by excessive data collection or unfair trading conditions, and must clearly establish a theory of harm to competition. Commenting on the OLG decision, Podzun noted that the Bundeskartellamt's 2019 decision had failed to meet the court's test regarding the theory of harm.¹¹⁹ According to Podzun, perhaps, the Bundeskartellamt would:

Have done itself a favour if it had gone much further and if it had brought up the courage to say: Yes, we are trying a novel theory of harm here! This is antitrust law for the digital age! And we are now seriously trying to take exploitative abuses to the spotlight after decades of ignorance.¹²⁰

The conflicting reasoning between the Bundeskartellamt and the OLG on the causality requirement highlights the importance of the test for competition agencies, as digital platforms would argue for a conduct causality requirement in their defense. Following the OLG's

¹¹⁵ Hausfeld, 'Abrupt End to "Hipster Antitrust"? Tackling Facebook's Expansion Following the First Court Ruling in Germany (20 November 2019, Hausfeld).

¹¹⁶ Mark-Oliver Mackenrodt, 'Germany' in Bruce Kilpatrick, Pierre Kobel and Pranvera Këllezi, *Antitrust in Data Driven Markets & Legal Framework for Influencers, Native Advertising and Control over the Use of AI in Marketing* (Springer 2023) 145-169, 159.

¹¹⁷ D'Amico above n 35 at 615.

¹¹⁸ OLG Decision, English version page 17.

¹¹⁹ Rupprecht Podzun, 'Facebook Vs. Bundeskartellamt' (D'Kart Antitrust Blog, August 30 2019)).

¹²⁰ Ibid.

decision, the Bundeskartellamt appealed to the Bundesgerichtshof, the German Federal Court of Justice (FCJ).¹²¹

4.3 Bundesgerichtshof Decision

The FCJ decision also contributed to identifying anti-competitive conduct, developing the theory of harm, and establishing the causality requirement.

a. Identifying the anti-competitive conduct

To the FCJ, the Bundeskartellamt and the OLG had rightfully found that the use of unlawful terms and conditions by a dominant undertaking can constitute an abuse of that undertaking's dominant position in accordance with Section 19(1) of the GWB.¹²² What is unique about the FCJ decision is that the FCJ did not focus solely on Facebook's data processing terms of use as a data breach; it took a competition-oriented approach, analyzing how those terms affected competition. Hence, the FCJ found that Facebook's conduct led to negative anti-competitive effects in its vertical relationship with users, in the form of exploitative abuse. In the horizontal dimension, Facebook engaged in exclusionary conduct by restraining actual or potential competition on the market for social networks.¹²³ The FCJ therefore confirms this paper's argument that the data processing terms of use of digital platforms become a competition concern when they are prohibited under competition legislation.

b. Developing a theory of harm

The FCJ rejected the OLG's finding that Facebook had not abused its dominant position because the users suffered no monetary harm and had a choice. In agreement with the OLG, the FCJ pointed out that it is true that 'Facebook does not cause its users economic harm, since data are an immaterial, non-rival, non-excludible and wear-proof resource'.¹²⁴ The FCJ, however, pointed out that this does not render competition law obsolete because 'the fact remains that by allowing Facebook to gather and commercially process their private data, users provide Facebook with a resource of economic value'.¹²⁵ In the FCJ's view, advertisers pay Facebook to analyze user data, generating revenue for the Company on the other side of the market.¹²⁶ Additionally, the user data Facebook collects gives it a competitive advantage because users contribute to a data pool created by Facebook and therefore available only to

¹²¹ Bundesgerichtshof, KVR 69/19.

¹²² Ibid, paras 14-16, 36.

¹²³ Ibid, para 64.

¹²⁴ Ibid para 61.

¹²⁵ Ibid.

¹²⁶ Ibid, para 59.

Facebook and its customers on the other side.¹²⁷ It is up to Facebook's discretion whether to share data with other platforms and not the users. Hence, the OLG could not argue that Facebook users have a choice to share data with multiple platforms.

Furthermore, in relation to the question of whether German Facebook users suffered harm in the form of limited choice, the FCJ, taking a competition-oriented approach, submitted that, as long as there were no effective competition and Facebook forced users to accept terms for the conditional use of its platform, users had no choice because their decision was not based on an autonomous user decision. In explaining the lack of effective competition, the FCJ pointed out that in a two-sided market, where the exploitation of one market side by the intermediary is likely to also have an adverse impact on competition on the other market side, effective competition is undermined because of market tipping, network effects, and data network effects. To the FCJ, these strong network effects have created a 'strong lock-in effect and ultimately render users more willing to accept the disadvantages associated with using the social network'.¹²⁸ For instance, 85.8% of German Facebook users surveyed by the Bundeskartellamt said it is important for their friends to also use Facebook.

In demonstrating how a lack of effective competition in the German Facebook social networking market limited users' choice, the FCJ cited a Bundeskartellamt survey aimed at determining users' preferences regarding data collection. The survey results showed that 46% of German Facebook users revealed they would switch to an alternative service if they had to reveal less data.¹²⁹ Additionally, 38.5% of users were willing to pay for access to a social network if Facebook collected less data. Thus, under effective competition and without barriers to switching to alternative providers, in the FCJ's reasoning:

A more diverse offer on the market for social networks could be expected, taking account of users preferences in favour of more autonomy as regards the disclosure of data that provide an almost comprehensive idea of their online activities as a whole, and offering users a choice between using a network with a more personalized user experience (as offered by Facebook with the processing of "off-Facebook" data) and a network that limits the personalization to the use of data gathered from the user's activities on the platform itself. Facebook does not offer its users this kind of choice.¹³⁰

In the FCJ's view, the OLG failed to consider 'the interests of those users that do not want to refrain from using Facebook but find it equally important that the collection and processing of their data is limited to what is necessary for the use and financing of the

¹²⁷ Ibid para 63.

¹²⁸ Para 44.

¹²⁹ Bundeskartellamt, 'Background Information on the Bundeskartellamt's Facebook Decision' (7 February 2019).

¹³⁰ Bundesgerichtshof decision, para 86.

network'.¹³¹ Furthermore, Facebook users are not given a choice about whether they want to use a social network that guarantees them a more personalized experience, but also allows Facebook to have unlimited access to information about their off-Facebook online activities. Or whether they only want to consent to a less personalized service. This observation would later shape the discussion of whether digital platform users should be given a choice between a less personalized experience limited to the data they share with the digital platform and a more personalized experience when they allow the digital platform to access data on and off the platform. To the FCJ, as long as a market lacks effective competition due to specific market characteristics, users' choices are limited, and this constitutes a harm to competition.

c. The causality requirement

The FCJ rejected the OLG's reasoning that, in cases of exploitative abuse, only conduct causality should be demonstrated, and agreed with the Bundeskartellamt that causality of results was sufficient to prove abuse of dominance. In particular, the FCJ noted that contrary to the OLG, 'an abuse of a dominant position does not always require a direct causality between the dominant position of the company and its ability to impose terms which result in an exploitation of customers'.¹³² In the FCJ's reasoning, competition agencies can demonstrate a causal link between a firm's market dominance and user exploitation by showing that the firm *leveraged* its market position to exploit users without needing to prove a direct cause-and-effect relationship, especially where effective competition would not occur due to specific market conditions. Thus, as stated by the FCJ:

A causal link between the dominant position and a specific market result (*result causality*) can be sufficient where, *on account of specific market conditions*, the conduct of the dominant company leads to market results that *would not be expected in a competitive market*, and where the *condemned conduct is not only exploitative but also liable to impede competition*.¹³³ (Emphasis added).

d. Analysis

Whether the FCJ's reasoning on causality, prioritizing result causality over conduct causality, can be applied by other competition agencies is debatable. In German, according to Mackenrodt, it is uncontested that 'a quite lenient causation requirement applies' in exclusionary conduct.¹³⁴ However, in the context of exploitative conduct, causation is highly

¹³¹ Ibid, para 58.

¹³² Ibid, para 65.

¹³³ Ibid, para 65.

¹³⁴ Mark-Oliver Mackenrodt, 'Data Processing as an Abuse of Market Power in Multi-Sided Markets: The More Competition-Oriented Approach in the German Federal Supreme Court's Interim Decision KVR 69/19-Facebook' (2021) 70(6) GRUR International 562, 567.

contested, as some scholars advocate stricter requirements for it. In the FCJ decision, causality requirements were guided by the lack of effective competition in multi-sided digital markets, which was exacerbated by the market's characteristics. That is, a lenient causation requirement is justified to protect competition on the other side of the market. The fact that the causation requirement was contentious in the Facebook case in Germany indicates that competition agencies must take causation seriously.

Although the FCJ agreed with the Bundeskartellamt on the result causality, some scholars have noted that the FCJ differed from the Bundeskartellamt's decision in several respects.¹³⁵ The Bundeskartellamt focused on excessive data collection and unfair trading conditions as a form of exploitative abuse. In fact, as illustrated by Mackenrodt, the Bundeskartellamt's line of argument primarily focused on the finding that Facebook's general terms and conditions were in conflict with data protection law, and the 'unilateral imposition of these contractual conditions on users constituted an abuse of market power in the form of qualitative exploitative abuse'.¹³⁶ Although the FCJ did find exploitative abuse, it focused more on exclusionary conduct in its analysis.¹³⁷ Additionally, commenting on the FCJ's decision, Mackenrodt notes that, compared to the Bundeskartellamt decision, the FCJ's theory of harm is more competition-oriented and does not derive the exploitative abuse from a mere violation of the GDPR.¹³⁸

Arguably, the FCJ examined Facebook's conduct solely under competition law, determining whether, in a competitive market, alternative firms offering users the opportunity to provide less data existed, and how this undermined users' choices. Mackenrodt argues that, in taking a competition-oriented approach, the FCJ decision sought to minimize any intrusion with the data protection regime by showing that 'a possible illegality of the general terms and conditions or an actual violation of the GDPR is no longer a necessary condition for finding an abuse'.¹³⁹ In agreement with the FCJ decision, Kerber and Zolna also state that, 'if we take into account, in competition law, the negative effects of competition problems on the privacy of consumers...the infringement of data protection law is neither a sufficient nor necessary condition for the abusive character of the behaviour of a dominant firm'.¹⁴⁰ Thus, not every data protection law breach by a dominant firm should be viewed as abusive behavior in

¹³⁵ Bundesgerichtshof decision, para 565.

¹³⁶ Ibid para 565.

¹³⁷ Alessia D'Amico, 'The Boundary Between EU Competition Law and the GDPR After Meta' (2024) 61 Common Market Law Review 787.

¹³⁸ Mackenrodt above n116.

¹³⁹ Ibid at 160.

¹⁴⁰ Kerber and Zolna above n37, at 238.

competition law. A data breach can serve as evidence of anti-competitive conduct. The role of the competition agency is to determine whether the conduct constitutes exploitative or exclusionary behaviour under competition law.¹⁴¹

After the FCJ decision, the OLG referred seven preliminary questions to the Court of Justice of the European Union (CJEU) for interpretation. The CJEU made its decision on 4 July 2023. At the time, Facebook was under Meta, so the case is referred to as *Meta vs Bundeskartellamt*.¹⁴² Before examining the CJEU's decision, a key development occurred in the EU prior to 2023. While the case was pending at the CJEU, the EU took a significant step in its technology governance by adopting the EU Digital Markets Act (DMA), which entered into force on 1 November 2022.

The DMA is ex ante legislation aimed at enhancing contestability and fairness in the EU single market by regulating the conduct of designated digital gatekeepers that meet the qualitative and quantitative thresholds set out in Article 3 of the DMA.¹⁴³ It is well recognized that the Bundeskartellamt/Facebook decision influenced the adoption of Article 5(2) of the DMA, which requires digital gatekeepers to procure user consent before processing their personal data. As Facebook is one of the designated digital gatekeepers under the DMA, it is crucial to briefly analyze Section 5(2) of the DMA to understand whether it addresses some of the issues raised in the Bundeskartellamt, OLG, and FCJ decisions, and whether the CJEU also relied on the DMA in its decision.

4.4 Article 5(2) of the DMA and Consent

Article 5(2) of the DMA prohibits designated digital gatekeepers from processing, combining, cross-using personal data of end-users using their services or end-users' personal data from third parties using their core platform services, unless the end-user is presented with a choice and provides consent as required under Article 4(11) and 7 of the GDPR. A digital gatekeeper cannot cross-use data from its digital ecosystem without the user's explicit consent. Amazon, for example, as a designated digital gatekeeper, cannot cross-use end users' personal data across its services—including Amazon Marketplace, Amazon Prime Music, Amazon Prime Video, and Amazon Prime Games—without the user's consent. Digital gatekeepers are also prohibited from signing end users up for other services provided by the gatekeeper, with the objective of combining data without the user's consent. For instance, Google cannot sign in

¹⁴¹ Martinez above n106.

¹⁴² CJEU, Case C-252/21

¹⁴³ European Commission, 'Gatekeepers' Available at https://digital-markets-act.ec.europa.eu/gatekeepers_en accessed 24 September 2025.

end users across all its core platform services without presenting them with a choice and obtaining their consent. This provision reduces the number of scenarios in which consent is bundled.

a. Anti-competitive conduct

That being said, from a broader perspective, the DMA views data accumulation by digital gatekeepers as a barrier to entry and a means to incentivize exclusionary conduct, limiting market contestability.¹⁴⁴ Recital 36 of the DMA acknowledges that the accumulation of personal data by digital platforms from their end-users and from third parties using their core platform services increases the digital gatekeeper's data accumulation, thereby raising barriers to entry. Furthermore, digital gatekeepers have the advantage of accumulating personal data from a significantly larger number of third parties than any other undertaking. Thus, the DMA views data accumulation as a source of power. As discussed in this paper, the accumulation of data by digital platforms leads to data power, which in turn increases other forms of platform power, such as digital ecosystem, bargaining, intermediary, and market power. While the DMA doesn't explicitly refer to the term 'exploitative conduct', the lack of valid consent in the processing of personal data by digital gatekeepers is seen as a deviation from the goal of fairness in how users are treated.

b. Data-related theory of harm

By requiring designated gatekeepers to obtain user consent in the processing of personal data, the DMA acknowledges users' right to choice and autonomous decision-making over their data. Recital 36 of the DMA also prohibits digital gatekeepers from 'making the use of the core platform services or certain functionalities thereof conditional upon the end user's consent'.¹⁴⁵ The DMA does not introduce a new notion of consent but rather relies on the GDPR. Actually, the application consent in the DMA is "without prejudice" to the GDPR, which means that the application of Article 5(2) of the DMA will not prejudice the rights existing under the GDPR.¹⁴⁶ Nevertheless, there is still debate on whether consent under the DMA the same as consent under the GDPR is, which is based on the "without prejudice" concept. Van de Waerdt argues there is no value Article 5(2) adds to the GDPR, and in fact, 'it could be argued that the GDPR is

¹⁴⁴ DMA, recital 3.

¹⁴⁵ Ibid, recital 37.

¹⁴⁶ See Konstantina Bania, 'Fitting the Digital Markets Act in the Existing Legal Framework: The Myth of the Without Prejudice Clause' (2023) 19(1) European Competition Journal 117.

already stricter than the new art.5 DMA aims to be.’¹⁴⁷ Despite this debate, competition agencies need not introduce their own notion of consent but rely on the notion provided in their data protection legislation to avoid divergence or reinventing the wheel.¹⁴⁸

Regarding the harm users face when consent to the processing of their personal data is not obtained, the DMA identified a lack of user choice as a form of harm, reflecting the decisions of the Bundeskartellamt and the FCJ. Furthermore, to enhance users’ choice, the DMA requires designated digital gatekeepers to ‘enable end users to *freely choose to opt-in to* such data processing and sign-in practices by offering a less personalized but equivalent alternative’.¹⁴⁹ This provides the end-users with two choices: consent to the processing of personal data or an alternative that is less personalized but equivalent.¹⁵⁰ A less personalized but equivalent alternative under the DMA aims to increase users’ choice and autonomy in how their data is processed. It also seeks to ensure that consent is not conditional on access to and use of the digital platform, and that withdrawal of consent is not detrimental, as required under Article 4(11) of the GDPR. This provision, however, raises a complex question regarding what constitutes a less personalized but equivalent alternative.

In addition to the lack of choice as a harm, the DMA also recognizes quality degradation as a user harm, as emphasized by the Bundeskartellamt. Under Recital 37 of the DMA, the less personalized service but equivalent alternative, ‘should not be different or of degraded quality compared to the service offered provided to end users who provide consent’. The DMA Recital 37, further, provides that where the quality of the less personalized, but equivalent alternative, service is of *lower quality* than the core platform service, the degradation of quality should be ‘as a direct consequence of the gatekeeper not being able to process such personal data or signing in of end users’. One can infer from this information that the personal data for which consent is obtained is necessary for the performance of the contract, so that if the end user does not grant consent to process the data, the service quality degrades. In this case, a digital platform can justify the degradation of its service quality due to limited access to personal data.

The DMA further requires that ‘at the time of giving consent, and only where applicable, the end user should be informed that not giving consent can lead to a less personalized offer, but otherwise the core platform service will remain unchanged and that no

¹⁴⁷ Peter J van de Waerdt, ‘Reinforcing Data Protection and Competition Through Art. 6(2) of the Digital Markets Act’ (2025) 82 International Review of Law and Economics 106265, 10.

¹⁴⁸ Alessia S D’Amico, ‘The DMA’s Consent Moment and Its Relationship with the GDPR’ (2025) 16 European Journal of Risk Regulation 170, 180.

¹⁴⁹ DMA, recital 36.

¹⁵⁰ DMA, recital 36.

functionalities will be suppressed’.¹⁵¹ This ensures that end users can choose between the less personalized and the personalized versions. Since the DMA entered into force on May 2, 2022, the interpretation of a less personalized but equivalent alternative remains largely contested. Some scholars have interpreted it to mean an ‘equal equivalent’ or a ‘truly equivalent service’.¹⁵² While others have questioned whether an equivalent alternative under the DMA requires the users to pay a monetary fee. This issue is not the subject of this paper.¹⁵³

c. Causality requirement

The DMA is not a competition legislation and does not have a causal requirement. Once the designated gatekeepers meet the criteria, the proof of dominance is not necessary. Hence, the causal requirement between dominance and conduct is not required.¹⁵⁴

4.5 CJEU Meta Platform v Bundeskartellamt

After the FCJ decision that rejected the OLG’s reasoning, the OLG referred seven preliminary questions to the CJEU for interpretation. The first question concerned whether a competition agency has the competence to determine and penalize a breach of the GDPR regarding the processing of personal data, and whether it has an obligation to cooperate with a data protection authority. The second question pertains to the conditions under which users’ consent to the processing of sensitive personal data is required, as prohibited under Article 9 of the GDPR. The third, fourth, and fifth questions required the CJEU to determine the lawfulness of Facebook’s processing of personal data under Article 6 of the GDPR, based on legitimate interests and the performance of a contract.

The sixth element of the preliminary question concerned the validity of consent to the processing of personal data provided to an undertaking with a dominant position. The seventh question asked whether a competition authority can, in the context of examining an abuse of dominant position by an undertaking within the meaning of Article 102 of TFEU, find that the undertaking’s general terms of use relating to data processing do not comply with the TFEU. While these questions are interesting, for the purposes of this paper, it will focus on the CJEU’s reasoning regarding when a data competition breach becomes a competition concern. The CJEU made its decision on 4 July 2023

¹⁵¹ DMA, recital 37.

¹⁵² Alexandre De Streel and Giorgio Monti, ‘Data-Related Obligations In the DMA’ (Centre on Regulation in Europe (

¹⁵³ See Sangjun Nam and Youngsun Kwon, ‘Is Pay-or-Consent for Privacy Justifiable? Evidence from Different User’s Privacy Attitudes Toward Behavioral Data Collection in South Korea (2024) 48(7) Telecommunications Policy 102794.

¹⁵⁴ Boistein

a. Can competition agencies consider a data protection breach?

The CJEU was of the view that in the context of examining an abuse of dominant position by a firm in a specific market, ‘it may be necessary for the competition authority of the Member State concerned also to examine whether the undertaking’s conduct complies with rules other than those relating to competition law’.¹⁵⁵ The CJEU therefore reiterated that a competition authority can use a data protection term of use as a *vital clue* to establish whether a firm with a dominant position abused its dominant position through its data processing terms, distorting effective competition.¹⁵⁶ More precisely, the CJEU reasoned that:

In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a *vital clue* among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers.¹⁵⁷ (emphasis added).

The above aspect of the CJEU reasoning – which is fundamental in addressing the tendentious relationship between data protection and competition law – implies that a violation of data protection law can serve as critical evidence for a competition agency to infer that a dominant firm has abused its dominant position and distorted effective competition.¹⁵⁸ In the CJEU’s view, access to personal data and the ability of digital platforms to process that data for profit have ‘become a significant parameter of competition between undertakings in the digital economy’.¹⁵⁹ Thus, ‘excluding the rules of personal data from the legal to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development’.¹⁶⁰ This observation aligns with the discussion in this paper, as well as with the Bundeskartellamt’s and FCJ’s reasoning, which highlight the role of data in enhancing a digital platform’s data power, thereby increasing its market dominance and making it a competition concern.

The CJEU decision also noted that there was no provision in the GDPR that prevents a national competition authority from performing their duties to find ‘data processing operation carried out by an undertaking in a dominant position and liable to constitute an abuse of that

¹⁵⁵ CJEU Case C-252/21, para 48.

¹⁵⁶ Adv. Rantos Opinion, point 23.

¹⁵⁷ CJEU Case C-252/21, para 47.

¹⁵⁸ For scholarly work interpreting the CJEU decision in the Meta Platforms/Bundeskartellamt, see, Leonardo Parona, ‘Addressing the Interplay Between Competition Law and Data Protection Law in the Digital Economy through Administrative Cooperation: The CJEU Judgment in the Meta Platforms Case’ (2024) 16(1) Italian Journal of Public Law 239; Giuseppe Colangelo, ‘The Privacy/Antitrust Curse: Insights from the GDPR Application in Competition Law Proceedings’ (2024) 70(1) The Antitrust Bulletin 113.

¹⁵⁹ CJEU Case C-252/21, para 51.

¹⁶⁰ Ibid para 51

position does not comply with that regulation.’¹⁶¹ This is despite the fact a data protection and competition authorities perform different functions and pursue their own objectives and tasks.¹⁶² Accordingly, the CJEU made it clear that a competition authority may rely on a breach of another regulation only for the sole purpose of determining an abuse of dominant position; it does not replace the authority of the other regulatory body.¹⁶³ Neither, as Parona observes,¹⁶⁴ does it imply that the competencies attributed to the latter authorities shall be extended. In cases where a competition authority is considering a data protection breach in assessing a firm’s abuse of a dominant position, the CJEU has called on competition authorities to cooperate with data protection authorities to ensure the consistent application of data protection legislation.¹⁶⁵

Some scholars have argued that the CJEU decision was not conclusive in addressing when a data breach becomes a competition law concern, as the CJEU failed to establish a specific threshold for determining when data can be a vital clue in assessing whether a firm has abused its dominant position.¹⁶⁶ It is worth noting that although the accumulation of data by a few tech companies draws the attention of competition agencies, it is essential that they establish clear thresholds for determining when a data protection breach constitutes sufficient evidence of anti-competitive conduct. To be more explicit, not every data breach implies a competition violation.¹⁶⁷ But what is undeniable is the fact that data processing terms can only be used as an important criterion in a more comprehensive assessment of a digital platform’s violation of competition law.

b. Identifying anti-competitive conduct

The OLG did not ask the CJEU to determine whether Facebook’s conduct was exclusionary or exploitative. Nonetheless, the CJEU addressed the issue of when data collection is necessary for the performance of the contract. Its reasoning is critical in informing competition agencies that seek to show that a digital platform has engaged in excessive data collection or unfair trading conditions. The CJEU introduced two guiding principles to determine whether data collection is extensive and unnecessary: objectively indispensable, and users’ reasonable expectations.

¹⁶¹ Ibid para 43.

¹⁶² Ibid para 44.

¹⁶³ Ibid para 49.

¹⁶⁴ Parona above n158, at 253.

¹⁶⁵ Paras 52.

¹⁶⁶ Colangelo above n158.

¹⁶⁷ Gorecka above n12 at 18.

Objectively indispensable

Regarding the question of whether the data collected by Facebook was necessary for the performance of its contract, the CJEU held that such a defence can only be valid ‘only on condition that the processing is objectively dispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur’.¹⁶⁸ It has been argued that the CJEU introduced the principle of objectively indispensable, which can be interpreted to mean that the purpose for which personal data is collected and combined with sources outside a digital platform’s core service must be objectively necessary to the core purpose of the contract. The digital platform must, therefore, demonstrate ‘how the main subject matter of the contract cannot be achieved if the processing in question does not occur’.¹⁶⁹

Meta had argued that combining data across its platforms was important for the seamless use of the Meta group’s own services and for personalized advertising. Similar to the Bundeskartellamt’s reasoning, the CJEU submitted that data processing for personalized advertising was not a service integral to the contract for providing social network services between Facebook and its users, even if the personalized advertising was offered free of charge. Accordingly, there was no obligation for the users to ‘subscribe to the various services offered by Meta group in order to create a user account in the social network’.¹⁷⁰ Furthermore, the various products and services offered by Meta Group can be used independently of one another, and each product or service is subject to a separate user agreement.¹⁷¹ In the current case, Meta had failed to demonstrate that such a data combination was necessary to provide its users with the services of the online social network.¹⁷²

The CJEU further pointed out that even when data processing is objectively indispensable to the provision of a specific service, the digital platform must also prove that there were no less privacy-intrusive alternatives.¹⁷³ The CJEU found Facebook’s conduct of combining on and off-Facebook data extremely privacy-intrusive and stated that:

The processing at issue in the main proceedings is particularly extensive since *it relates to potentially unlimited data* and has a significant impact on the user, a larger part –if not almost all– of whose online activities are monitored by Meta Platforms Ireland,

¹⁶⁸ CJEU Case C-252/21, Para 125.

¹⁶⁹ Ibid para 98.

¹⁷⁰ Ibid para 103.

¹⁷¹ Ibid para 103.

¹⁷² Ibid para 102.

¹⁷³ Ibid para 99.

which may give rise to the feeling that his or her private life is being continuously monitored.¹⁷⁴ (Emphasis added).

It is at this point that the CJEU interpreted the ‘excessiveness’ of Meta’s data processing terms in absolute terms rather than quantitatively by introducing the principle of objectively indispensable. This implies that, in assessing the “excessiveness of data collection” by competition agencies, they should consider whether the data processing was necessary for the performance of the main subject. This is particularly critical in markets with a digital ecosystem, such as those offered by Meta, Amazon, Google, and Apple. If a digital platform intends to use data for any purpose other than its original intended use, it must obtain separate consent.

Users’ reasonable expectations

Where a digital platform raises contract performance as a justification for data processing, the CJEU argued that users’ reasonable expectations must be taken into account, as well as the ‘scale of the processing at issue and its impact on that person.’¹⁷⁵ Although services of an online social network such as Facebook are usually free of charge, in the CJEU’s view, ‘the user of that network cannot reasonably expect that the operator of the social network will process the user’s personal data without his or her consent, for the purposes of personal advertising’.¹⁷⁶ Meaning that where a user did not expect excessive data collection for purposes not specified in the contract with a digital platform, the competition agencies can, from this lens, argue that such conduct constitutes an exploitative abuse, as it exceeds the user’s reasonable expectations.

c. Theory of harm

Regarding the theory of harm, as the Bundeskartellamt and the FCJ have, the CJEU also identified a lack of user choice as a potential harm. In the CJEU’s view, a digital platform’s dominant position creates an imbalance between the user and the platform, favoring the platform. Unfortunately, due to a clear power imbalance, Facebook users did not have the right to refuse consent to such extensive data collection on an individual basis. If the users opted out of Facebook’s data processing, they would be penalized by losing access to the service entirely.¹⁷⁷

To increase users’ choice, as the FCJ similarly argued, the CJEU held that they should be given a less personalized alternative. However, unlike the FCJ, the CJEU argued that users

¹⁷⁴ Ibid para 118.

¹⁷⁵ Ibid para 116

¹⁷⁶ Ibid para 117.

¹⁷⁷ Ibid para 150.

should be offered, ‘if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.’¹⁷⁸ This CJEU observation aligns with Recital 37 of the DMA, which requires digital gatekeepers to provide users with a less personalized but equivalent alternative. The CJEU, however, provides that such an alternative can be provided for an appropriate fee. The CJEU decision has raised controversy over whether the pay-or-consent model increases users’ choice.¹⁷⁹

d. Causality requirement

In its analysis, the CJEU did not rely on result causality, unlike the Bundeskartellamt and the FCJ, in the Meta/Bundeskartellamt case. The CJEU focused on establishing that a competition agency can show that a dominant digital platform abused its position through data processing terms of use that were prohibited by a data protection legislation.¹⁸⁰ Endorsing Advocate General Rantos’ opinion, which held that a dominant position is necessary but not sufficient in itself to cause exploitative abuse in digital markets.¹⁸¹ However, in agreement with the Bundeskartellamt and FCJ decisions, the CJEU argued that a firm’s dominance must be taken into account when determining whether users’ consent was freely given, because ‘that circumstance is liable to affect the freedom of choice of that user who might be unable to refuse or withdraw consent without detriment, as stated in recital 42 of the GDPR’.¹⁸²

Scholars have interpreted the CJEU’s decision in the Meta/Bundeskartellamt case to mean that competition agencies must demonstrate a direct causal link between the data protection breach under the GDPR and the abuse of a dominant position when integrating a data breach into competition law assessments. In other words, this could mean that, were it not for the data protection violation, an abuse of dominance would not have been found. The question relating to causality requirement, especially when it comes to exploitative abuse, which in many countries adopts conduct causality, will depend on each jurisdiction’s practice.

5.0 Reflections, Analysis, and Conclusion

The reason this study is important is that data is now a critical consideration in assessing competition law violations. This is evidenced by the increasing investigations by competition agencies in data-related terms of use. After the Bundeskartellamt, an increasing number of

¹⁷⁸ Para 150.

¹⁷⁹ D’Amico above n35.

¹⁸⁰ Inge Graef, ‘Meta Platforms: How the CJEU Leaves Competition and Data Protection Authorities with an Assignment’ (2023) 30(3) Maastricht Journal of European and Comparative Law 325.

¹⁸¹ AG Rantos Opinion, Para 77.

¹⁸² Para 148.

competition agencies –the French Autorité de la Concurrence (FCA), the Argentine National Commission for the Defense of Competition (CNDC),¹⁸³ the Nigerian Federal Competition and Consumer Protection Commission (FCCPC), the Chilean Fiscalía Nacional Económica,¹⁸⁴ and the Competition Commission of India (CCI)–¹⁸⁵ have investigated digital platforms’ data processing terms of use. These competition agencies have had to grapple with the same challenges as the Bundeskartellamt/Facebook decision, for example, identifying anti-competitive conduct, conceptualizing it, developing a theory of harm, and demonstrating the causality requirement. Importantly, these competition agencies have been accused of encroaching on data protection regulations.

Legislatively, in 2022, the EU Digital Markets Act (DMA) incorporated Article 5(2), which prohibits designated digital gatekeepers from processing personal data without the user’s consent. Similar provisions to Article 5(2) of the DMA have been introduced in new digital market competition regulations (DMCR) adopted in other countries. For instance, Section 20 (3g) of the UK Digital Markets Competition and Consumer Protection Act (DMCCA) prohibits designated firms with strategic market status from using data unfairly. This provision can be interpreted to mean that firms with strategic market status should not combine or cross-use data from other platforms without the user’s consent. In Africa, Article 11(4h) of the African Continental Free Trade Area (AfCFTA) Competition Protocol prohibits designated gatekeepers from combining personal data sourced from different services offered by the gatekeepers.¹⁸⁶

The above legislative developments and competition agencies’ investigations into digital platforms’ data-related terms of use show that in the era of the digital economy, where data serves as the infrastructure that determines the success of tech companies’ business models, it is practically undeniable to advocate for a firewall between competition and data protection regulation. Furthermore, most of the competition agencies’ investigations have involved similar global tech companies. If the Bundeskartellamt/Facebook decision continues to influence global regulatory responses in determining when data-related terms of use, especially regarding valid consent, then an in-depth analysis of the Bundeskartellamt, OLG, FCJ, and the CJEU decisions provides a starting point for competition agencies faced with similar regulatory challenges. A summary of this study’s findings are discussed below:

¹⁸³ Canales and de Souza above n60.

¹⁸⁴ Manuel Abarca, ‘The Chilean Case Against WhatsApp’ (Kluwer Competition Law Blog, 8 October 2025) <https://legalblogs.wolterskluwer.com/competition-blog/the-chilean-case-against-whatsapp/> accessed 14 October 2025.

¹⁸⁵ CCI, ‘CCI Imposes a Monetary Penalty of Rs. 213.14 Crore on Meta for Anti-Competitive Practices in Relation to 2021 Privacy Policy Update’ (CCI Press Release No.71/2024).

¹⁸⁶ See also the Bundeskartellamt against Google for its data processing

a) Data as a parameter of competition

Data is a source of digital platforms' market dominance, hence a non-price parameter when assessing a digital platform's market power. Despite the role of data as a parameter of competition, a violation of data protection law does not automatically become a concern under competition law. Neither should a breach of data protection law be used as the sole benchmark for identifying the abusiveness of data-collecting practices and privacy terms.

b) Legal basis of investigating a digital platform's data processing terms

Competition agencies should focus on identifying competition violations resulting from the data processing terms of use of digital platforms. This provides competition agencies with the legal basis for invoking an investigation into a digital platform's data-related terms of use. This approach does not preclude competition agencies from referring to other regulatory regimes, like the data protection law. Although the Bundeskartellamt focused more on exploitative abuse of Facebook's conduct in the form of excessive data collection and unfair trading conditions, the FCJ's decision has demonstrated that indeed data processing terms of use can also lead to exclusionary conduct

c) Assessing the legal test of anti-competitive conduct

Regardless of the anti-competitive conduct it relies on, a competition agency must demonstrate that it meets the legal test under the competition law assessment. For instance, the Facebook case has clearly revealed the challenges of conceptualizing excessive data collection in quantitative terms, particularly in a multi-sided market where users do not pay a price to access the digital service. This paper hypothesized that in such a case, data collection is likely to be "excessive" if the data collected by a digital platform is used for a purpose other than that for which the user originally consented. The Bundeskartellamt, FCJ, and CJEU decisions have affirmed this hypothesis and shown that linking a digital platform's data processing terms to specific contract performance can provide competition agencies with an opportunity to determine the excessiveness of data collection, if it can be shown that the extensive data processed was not objectively indispensable and it failed to reflect users' reasonable expectations.

d) Developing a competition harm

While generally data processing terms of use fall under data protection law and lead to a privacy harm, the Bundeskartellamt, FCJ, and CJEU decisions, in addition to emerging scholarly work and Article 5(2) of the DMA, a privacy harm can be incorporated in competition assessment where it can be shown that it has affected effective competition,

and consequently led to user harm in the form of lack of user choice and degraded product quality. Competition agencies, therefore, can consider privacy-related harms as a parameter of non-price competition harm only when the privacy harm is linked to competition harm. The privacy harm identified by the competition agency in digital markets, however, must be a type of harm that is a concern for competition law, such as increased product prices, reduced consumer choice, reduced product quality, and reduced innovation. Hence, it is up to the competition agencies on a case-by-case basis to demonstrate how a digital platform's data processing terms of use have led to competition harm.

e) Causality requirement

The issue regarding the causality requirement, as addressed by the Bundeskartellamt, the OLG, the FCJ, and the CJEU, especially in relation to exploitative conduct resulting from a digital platform's data processing terms of use, remains contentious. Yet, it is very important for competition agencies to show whether a strict causal link between the exploitative conduct and the harm suffered by users should be shown. Or whether, by mere proof of market dominance, they can argue that the harm resulted from the digital platform's dominance.

f) Causal link between data breach and competition law

At the onset, this paper argued that if competition agencies take a competition-oriented approach that focuses on the digital platform's conduct and whether it is prohibited under competition law, whether such conduct is a data breach, or an AI Act breach, is not central to a competition agency's decision to investigate and assess competition concerns relating to a digital platform's conduct. In the digital economy, many regulatory areas will have a nexus with others. Hence, it is important that regulatory agencies focus on the legal basis of any investigation they undertake, and other areas could be used to infer violations within their specific legislation. Seen in this view, this approach will shield regulatory agencies from having to first determine if a violation under another legislation constitutes a violation in their legislation, and ultimately limits jurisdiction conflicts, conflicting decisions, and conflicts of law. For instance, a lack of valid consent in the processing of personal data by a digital platform can be used by competition agencies as evidence to infer that the processing terms of use, which require conditional access to a digital platform based on consent to extensive data processing collection, are an unfair trading condition, especially in markets without effective competition.