DIPARTIMENTO DI ECONOMIA E FINANZA

Cattedra di IO & Competition Theory

DATA-DRIVEN DOMINANCE: EXPLORING THE ROLE OF PLATFORMS AS *DE-FACTO* PRIVACY REGULATORS IN THE RECENT *APPLE ATT* AND *GOOGLE SANDBOX* CASES

RELATORE
Antonio Buttà

CANDIDATO
Federica Maria Vurro
Matr. 276771

ANNO ACCADEMICO 2023/2024

TABLE OF CONTENTS

1. Introduction

We currently live in a dynamic era characterized by remarkable innovation and transformation. The advent of digitization has fundamentally reshaped the landscape of data generation, storage, processing, exchange, and dissemination. In combination with the Internet, digitization has led to the emergence of new possibilities and *business models*. Moreover, advancements in artificial intelligence (AI) have further expanded the horizon of potential technological opportunities, fostering new avenues for innovation and presenting profound societal and economic prospects. As data and information serve as the cornerstone of nearly all societal and economic interactions, the revolution in their organization and transmission has had a profound impact on our daily lives. The accessibility of information has undergone a significant surge, owing in part to the rise of novel information intermediaries. This surge has facilitated cross-border transactions for both individuals and businesses, while concurrently enhancing consumer choice. Digitization is impacting every industry, spanning from manufacturing to services to agriculture.

However, alongside the numerous benefits digital innovation offers, the enthusiasm and optimism that defined the early years of the Internet have waned, giving rise to concerns and skepticism. Fears loom large, including worries about data theft and privacy breaches, the displacement of human labor by machines, the consolidation of economic power within a handful of ecosystems and platforms, and the exacerbation of economic inequality through new technologies. In the early 21st-century economic literature, it was commonly assumed that online competition would flourish as consumers browsed different websites, easily comparing offerings. However, reality unfolded quite differently. Even in the early days of the Internet, only a handful of "gateways" emerged. Fast forward to today, a few ecosystems and large platforms have become the primary gateways through which people access the Internet. And indeed, as of March

2024, the largest firms in the world by market capitalization are in the digital sector: Microsoft, Apple, Nvidia, Alphabet (Google), and Amazon[1].

Furthermore, certain platforms are deeply integrated into ecosystems of services and devices, creating a seamless complementarity among them.

The widespread influence of major digital platforms in our daily lives, their continual expansion beyond their initial markets, and their entrenched market power, have raised concerns in various quarters.[2] The impact of these gateways extends beyond purely economic realms and encompasses social and political issues, including concerns related to consumer data protection.[3] Personal data and its use have become the front-line of businesses in the digital market.[4] With the potential to extract information and make it available for various purposes, big data represents a powerful tool for data controllers, facilitating effective marketing strategies, informing strategic business decisions, and establishing a strong market foothold. [5]

The use of personal data for targeted marketing serves as a prime example of this. While privacy has been subject to the regime of privacy protection, privacy violations might entangle competition law analysis when they involve abuse of market dominance. [6] While data protection primarily focuses on safeguarding the interests of users as data subjects, competition law takes a different approach. Although the aim of both realms is to benefit consumers, competition law primarily seeks to ensure a level playing field in the market, by eliminating entry barriers and fostering free and effective competition. [7]

Numerous countries have contemplated, and in some instances implemented, legislative initiatives aimed at regulating Big Tech companies. In tandem with these efforts,

---

[1] CompaniesMarketCap.com. (March 18, 2024). Leading tech companies worldwide 2024, by market capitalization (in billion U.S. dollars) [Graph]. In *Statista*. Retrieved March 23, 2024, from https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/

[2] Motta, Massimo. "Self-Preferencing and Foreclosure in Digital Markets: Theories of Harm for Abuse Cases." *International Journal of Industrial Organization* 90, (2023): 102974.

[3] European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., Competition policy for the digital era, Publications Office, 2019, https://data.europa.eu/doi/10.2763/407537 [*hereinafter* Crémer Report]

[4] Wahyuningtyas, Sih Yuliana. "Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market." *European Business Organization Law Review* 18, no. 4 (2017): 785-800.

[5] *Id.*

[6] *Id.*

[7] *Id.*

antitrust agencies have intensified their actions, conducting market inquiries on some of their activities, scrutinizing their mergers, and opening abuse of dominance investigations into their practices. The type of abuse of dominance analysed in this study is often described with the term "self-preferencing", referring to situations in which an integrated platform "discriminates in favour of its first-party services or products to the detriment of those of a third party, e.g., by making the latter less prominent, ranking them lower, degrading or delaying their access to the platform, or worsening their terms and conditions of access. As such, they may result in partial or full exclusion." [8] Abuse of dominance is the most controversial area in competition policy, with very different enforcement standards in Europe and the US and differing views among lawyers and practitioners regarding the rationale behind exclusionary practices. This is especially notable in digital markets, which exhibit unique traits such as offering zero prices for consumers and experiencing rapid rates of innovation. These particular characteristics have led to skepticism regarding potential harm to consumers. [9]

Many of the online services that are driving the huge growth in the digital economy, are marketed as 'free' but in effect require payment in the form of personal information from customers. [10] Online advertising serves as the financial backbone of free online content and has burgeoned into a multi-billion-dollar industry since its birth in the 1990s. [11] Central to this industry is the capability to identify and track users through various technical means, such as web cookies. However, the practice of online tracking for advertising purposes has ignited privacy concerns and is subject to a growing body of regulation across the world. Yet, the most significant "regulations" appear to originate from a select few major technology platforms, notably Google and Apple. Operating as providers of the most widely used browsers and mobile operating systems, these companies have implemented a series of measures in the name of user privacy. These measures, aimed at limiting the ability to identify users, are fundamentally

[8] *Supra* note 2, at 2
[9] *Id.*
[10] Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy (Mar. 2014), available at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf
[11] Geradin, Damien, Dimitrios Katsifis, and Theano Karanikioti. "Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective." *European Competition Journal* 17, no. 3 (2021): 617-681.

reshaping the landscape of online advertising. [12]

In examining Google and Apple's influential role as *de facto* privacy regulators in the realm of online tracking, this study delves into Chrome's recent move to gradually eliminate support for third-party cookies. This initiative is complemented by a set of proposals dubbed the Privacy Sandbox. Additionally, the study scrutinizes Apple's implementation of the App Tracking Transparency Policy, a privacy-enhancing measure mandating stricter rules for competitors—namely, app developers reliant on the company's App Store—compared to those imposed on Apple itself.

Furthermore, an additional new and broad political debate has emerged both in Europe and the United States about the need for far- reaching reforms of competition policy, for example, through additional *ex-ante* regulatory solutions. [13] This discussion has been triggered in particular by far-spread serious doubts about the suitability and effectiveness of traditional competition law for solving the new challenges by the economic power of the large tech firms.[14] The "Digital Markets Act" (DMA) proposal of the European Commission, has established an ex-ante regulatory framework for large online platforms acting as gatekeepers, recognizing the power held by big platforms, which allows them to set the rules of the game and exercise control over whole ecosystems and provide regulatory oversight over these platforms. [15] In an era of rapid economic transformation, competition law demonstrates its adaptability by intervening intelligently and flexibly. This is particularly crucial as the fundamental shifts brought about by the data and platform economy poses challenges to many traditional regulations designed for addressing "old world" problems. Effective competition policy necessitates robust analysis of the evolving market dynamics and the identification of market failures.[16]

---

[12] *Id.*
[13] Kerber, Wolfgang. "Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law." *Antitrust bulletin.* 67, no.2 (2022): 280–301.
[14] *Id.*
[15] *Supra* note 11, at 37
[16] *Supra* note 3, at 14

Section 2 of this dissertation begins by outlining trends in the digital economy and examining the role of data as a potential source of competitive advantage. Furthermore, it provides an overview of the structural characteristics of digital platforms and elucidates how these features bolster the market power of Big Tech. In the third section, a framework for the analysis of abuse of dominance cases is constructed, delving into article 102 of the Treaty of the Functioning of the European Union. This section sheds light on the analytical challenges confronted by antitrust authorities in digital markets and explores the various facets of the interaction between antitrust enforcement and privacy. Particular emphasis is placed on integrating privacy considerations into the abusive practice of self-preferencing. Chapter 4 presents and analyses the two cases, CMA's Google Sandbox investigation and the Italian ACGM Apple ATT decision.
Section 5 provides a comprehensive overview of the relationship between data protection and competition law, summing up on the use of data privacy as a justification for anti-competitive conduct. Moreover, it examines the implications of the adoption of the Digital Markets Act in addressing cases of self-preferencing. Finally, section 6 concludes.

2. Exploring the digital economy

2.1) Key economic characteristics of digital markets

The Internet ecosystem is defined as an "internet-dependent, business-enabling system within the broader economy, defined by activities that rely on the internet to promote exchanges of products, services, and information."[17] Today, many believe the Internet is concentrated because Big Tech consists of digital platforms, while others argue that technology sectors, including the Internet, are too dynamic to remain beholden to monopoly power for too long. The former opinion challenges the long-standing theory of "creative destruction," which characterizes industrial change as incessantly revolutionizing the economic structure from *within,* incessantly destroying the old one,

[17] Creser, Olivia T. "In Antitrust we Trust? Big Tech is Not the Problem - it's Weak Data Privacy Protections." *Federal Communications Law Journal* 73, no. 2 (2021): 289-316.

incessantly creating a new one. [18] The Internet has undergone a significant transformation, shifting from a decentralized web to a landscape dominated by semi-closed platforms. This shift has attracted the interest of researchers and scholars who are eager to understand the underlying structural models that not only facilitated this transition but also empowered specific firms to capture and retain market power over time. [19]

A defining characteristic distinguishing Big Tech companies from other internet-based entities, lies in their nature as digital platforms. These platforms function as two-sided markets, where an intermediary – the platform itself – fosters interaction between two distinct yet interdependent user groups, typically buyers and sellers. Digital platforms are generally prone to tipping: once a firm gains enough users in a given market, it establishes itself as a powerful incumbent that is difficult to displace.[20] Indeed, experience shows that large incumbent digital players are very difficult to dislodge. From a competition policy point of view, there is also a reasonable concern that dominant digital firms have strong incentives to engage in anti-competitive behavior. All these factors heavily influence the forms that competition takes in the digital economy.[21]

Several key characteristics inherent to digital markets – extreme returns to scale, network externalities, and the crucial role of data – act as potent forces that amplify the market power of Big Tech companies.[22] These aspects, although not new in antitrust analysis, acquire particular relevance in digital markets, due to the significant conditioning effect their cumulative impact can exert on competitive dynamics, leading to high concentration and to the creation of *barriers to entry*. In the digital sector, high fixed costs—often exceptionally high and not recoverable (so-called "sunk costs"), as in the case of search engines and e-book distribution platforms—are accompanied by low or even zero *variable costs*.[23]

---

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Supra* note 3, at 3
[22] *Id.*
[23] AGCM, AGCom and Garante Privacy, Indagine conoscitiva *IC53 – Big Data*, (Dec. 20, 2019)

Moreover, the new technologies of information exhibit significant *returns to scale*: the cost of production is much less than proportional to the number of customers served.[24] While this aspect is not novel as such, the digital world pushes it to the extreme and this can result in a significant *competitive advantage* for incumbents. In industries characterized by increasing returns to scale, there is often a tendency toward concentration, where a few dominant firms capture a significant portion of the market. This concentration can lead to barriers to entry for new firms, as established players benefit from cost advantages and may have already captured economies of scale. Overall, competition with increasing returns to scale can result in a market structure where a few large firms dominate, potentially leading to less competition and higher barriers to entry for new entrants.[25]

The presence of large *economies of scale* also helps understand the rise of free services. There is some evidence that consumers are attracted by a *zero price*: there is an upward discontinuity in demand when the price reaches zero.[26] Firms face a strategic dilemma in deciding whether to charge for their services or distribute them for free, relying on advertising revenue. When economies of scale and the appeal of free services are strong enough, the latter option often becomes the preferred choice.

Another factor that renders the new information technologies incompatible with traditional modes of competition is their susceptibility to *network externalities* – the benefits derived from using a technology or service increase as the number of users grows.[27] Ultimately, the value of a network increases more than proportionally with its size. Large platforms are more efficient than smaller ones, leaving space for only a limited number of platforms in the market. Indeed, a large platform provides a more valuable service, e.g. access to more users for a one-sided platform, than a smaller one. Consequently, it is not enough for a new entrant to offer better quality and/or a lower

[24] *Supra* note 3, at 20
[25] *Id.*
[26] *Id.*
[27] *Id.*

price than the incumbent does; it also has to convince users of the incumbent to *coordinate* their migration to its own services. [28]

While incumbents benefit from increasing returns to scale primarily due to technological factors, the benefits of network externalities stem from the challenge users face in coordinating their migration to a new platform. Indeed, even if the users would all be better off if they migrated *en masse* to a new platform, they would not necessarily have an *individual* incentive to move to the new platform. Their decision to migrate hinges on their expectation that others will follow suit.[29]

A significant impediment to migration is represented by *collective switching costs*: various users find it difficult to coordinate to switch to an incompatible technology. This can occur, for example, due to the lack of interoperability between systems of competing operators, generating lock-in phenomena, or due to users' reluctance to switch providers because of significant network effects.[30]

Network effects, whether direct or indirect, may hinder a superior platform from supplanting an established incumbent. The magnitude of this "incumbency advantage" varies based on several factors, such as the feasibility of multi-homing, data portability, and data interoperability. When users have the option to use multiple platforms simultaneously, i.e. multi-homing, it becomes easier for a new entrant to persuade some users to switch to their platform while still retaining the benefits of using the incumbent platform to interact with others. [31]

A special case of network externalities has gained lots of attention since the beginning of the century: two-sidedness. A platform exhibits two-sidedness when it connects two different and well-identified groups of users. For two-sided platforms, the benefit that one side derives from the platform depends depends not only on the number but also on the identity of participants on the other side. Each side of the market is both a consumer of the platform, and the "product" which is being sold to the other side of the market. It

[28] *Id.*
[29] *Id.*
[30] Interoperability allows new entrants to offer services complementary to those offered by one or several platforms, facilitating multi-homing and allowing new entrants to grow and potentially challenge the dominance of a platform.
[31] *Id.*

is perfectly natural and can be pro-competitive for a platform to subsidize one side of the market when its presence on the platform is very valuable to the other side. For instance, platforms relying on advertising revenues will often provide content for a very low price, or even for free, to consumers, in order to attract them. [32]

The third, and arguably the most crucial aspect of digital markets, entrenching the market power of digital players, is the *role of data*, examined at length in the subsequent paragraph. Technological advancements have facilitated the collection, storage, and utilization of vast quantities of data, ushering in significant shifts in market dynamics. Data is one of the key ingredients of AI and smart online services, and a crucial input to production processes, logistics and targeted marketing. The ability to leverage data and to develop new, innovative applications and products is a competitive parameter whose relevance will continue to increase. Furthermore, since data is sometimes accumulated as a by-product of the normal functioning of a platform, incumbents will have access to much more and more recent data than other firms, and this will be a source of competitive advantage.[33]
A consequence of characteristics like network effects, increasing returns to scale and the role of data, is the presence of strong "economies of scope", which favor the development of *ecosystems* and give incumbents a strong competitive advantage. [34]

2.2) The Big Data Revolution: overview of the phenomenon

In pursuit of examining the fundamental characteristics of digital markets, bolstering the market power of platforms, the preceding discussion has centered on two pivotal aspects: network effects and increasing returns to scale. Yet, in recent years, another significant aspect of *platform economics* has risen to prominence: the role of data.

Data has become increasingly important in organizing production and exchange activities, to the extent that it can be considered an economic resource in its own right, indeed the most important resource in many sectors. Thanks to advancements in

[32] *Id.*
[33] *Id.*
[34] *Id.*

Information and Communication Technology (ICT), organizations tend to collect data of any type, process them in real-time to enhance their decision-making processes, and store them permanently for future reuse or knowledge extraction.[35] In this context, the term "Big Data" roughly refers to the collection, analysis, and storage of large quantities of data, including personal data. The massive nature of data processing operations necessitates that such information sets undergo automated processing through algorithms and other advanced techniques to identify probabilistic correlations, trends, and patterns.

Operationally, in the ICT sector, Big Data refers to a collection of data that cannot be acquired, managed, and processed by "traditional" computing tools, software, and hardware in a tolerable time, although there is no predefined dimensional threshold for data sets to be classified as Big Data. [36] Some recurring characteristics regarding the phenomenon are summarized in the 4 "Vs": *volume*, referring to the enormous size of generated and collected data; *variety*, concerning the numerous types of available data; *velocity* of processing operations; and the *value* that data assume when processed and analyzed. [37]

The data that is subject to processing can be personal or non-personal, a distinction that is relevant from a regulatory perspective. The General Data Protection Regulation (GDPR) [38] sets up a special framework for personal data, which grants important rights of control to individuals. Therefore, access to, respectively, personal and non-personal data follows different paths and needs to be discussed separately. The GDPR, which sets out when and how personal data may be processed, has far-reaching consequences for the way personal data can be accessed, traded and shared. It sets out a legal framework for the digital economy which shapes the functioning of markets and competition in all areas related to personal data. With regard to non-personal data, an

[35] *Supra* note 23, at 5.
[36] *Id.* at 7
[37] *Id.* at 8
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).

important debate on (non-competition law based) access rights has evolved; its outcome will have a substantial impact on markets for data and competition. [39]

Within the concept of "personal data", which is "any information relating to an identified or identifiable individual (data subject), both as a citizen and consumer", lies the concept of "consumer data" capturing data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship. At the same time, the term "consumer data" is also broader than "personal data" since it may also capture data concerning consumers even where such data cannot necessarily be traced to the individual. Consumer data are heterogeneous and non-rivalrous and can be classified in a number of ways: (i) by the *type* of data collected, (ii) by the *origin* of the data, or (iii) according to whether consumer data can be personally identifiable. When categorized pursuant to their origin, we can distinguish between volunteered, observed, inferred and acquired data.[40]

How data originates will affect consumer awareness of the data, and consumer awareness is important to addressing asymmetric information problems associated with the collection and use of consumer data. [41] Furthermore, this distinction has implications regarding the questions of whether the same information can be gathered or gained by competitors independently, or whether a dataset may be unique and access to it possibly indispensable to compete effectively.[42]

Personal data can also be classified according to the extent to which it is personally identifiable. We can distinguish four categories: identified, pseudonymised data, anonymised data and aggregated data. The relevance of this categorization is that where data cannot be attributed to an individual, it is less likely to trigger privacy laws. Hence,

[39] *Supra* note 3, at 77.

[40] Volunteered data are data that individuals provide when they explicitly share information about themselves or others. Examples include log in credentials, social media posts, and credit card information for online purchases. Observed data are created where an individual's activities are captured and recorded. Individuals create this data passively and sometimes unknowingly. Examples include location tracking and online browsing activities. Derived (or inferred) data are created from data analytics, including data that is derived mechanically from other data, as well as from more sophisticated techniques. Credit scores are one example. The individual is likely unaware of this data, and such data can be inferred even without much information being provided by the individual. Acquired (purchased or licenced) data are obtained from third parties through commercial licensing contracts (e.g. from data brokers) or non-commercial means (e.g. open government initiatives).

[41] Organisation for Economic Co-operation and Development (OECD), *Consumer Data Rights and Competition- Background Note* (2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.

[42] *Supra* note 3, at 75.

such data may be able to provide economic and competitive benefits without triggering offsetting privacy concerns.[43] A four-step 'personal data value chain' has been identified, consisting of (1) collection and access, (2) storage and aggregation, (3) analysis and distribution and (4) usage of personal datasets, which can be simplified to data i) generation and collection and ii) analysis and use. [44]

The Big Data collection phase begins with the generation, which occurs within activities carried out by users in a computerized environment or within the scope of the so-called Internet of Things. In the current context, where virtually all media content is available in digital format and a large part of economic and social activities has migrated online, user activities, both online and offline, can generate large amounts of data.[45]

When talking about the collection of consumer data, it is useful to distinguish between first and third party data collection. First party data collection occurs where a business collects information directly from its customers/users as part of their use of the business' goods or services. For example, Google's first party data is the data that Google collects from users when they are using all the services owned and provided by Google. In addition to the data it collects on its own websites and applications, Google also collects a wide range of data from third-party tracking of consumers on a range of (non-Google) websites and apps. It is noted that among application developers and/or website operators, it is common practice to outsource tracking systems developed by major ICT operators (such as Apple, Google, and Facebook), with the consequence that the data acquired by the former are also available to the latter, who, moreover, as developers of extremely widespread operating systems and/or extremely popular apps, are already in a privileged position for the direct acquisition of user data from smartphones and/or their applications. [46] Third parties may agree to such tracking as part of commercial agreements to receive website analytics and ad services, for example, as well as in using proprietary Application Programming Interfaces (APIs). Traditionally, "cookies"- text files that collect preferences (e.g., language, interface, location from which access occurs, etc.) and consumer information (e.g., pages visited,

[43] *Supra* note 41, at 9.
[44] *Supra* note 23, at 8.
[45] *Id.*
[46] *Id.* at 13-14.

texts transmitted, etc.) active on a website- allow precise profiling, which is updated on each subsequent access to the same site. Cookies can be first-party or third party. First-party cookies originate from (or are sent to) the website being visited, whereas third-party cookies originate from (or are sent to) an unrelated website. Third-party tracking is widespread across both websites and mobile apps. However, despite the numerous entities engaged in tracking, a significant portion of these trackers are controlled by a small number of data giants.

As previously stated, the way in which consumer data is collected has implications for privacy and competition. In respect of privacy, consumer awareness of data collection practices influences their ability to control their personal data. Specifically, consumers may feel most comfortable in relation to volunteered data that is collected and used directly by first parties. They might also feel relatively comfortable in respect of first party observed data. However, consumers may be less aware of data gathered through third-party tracking, even where consumers provide such data voluntary or where they are aware that their data is being observed by the relevant (first party) business.[47] Even when certain consumer data is easily collected in various ways and by various parties, access to third-party tracking, as well as a large and individually identifiable consumer base, may provide a business with a particularly *valuable set of data* that may be difficult for competitors to replicate. [48] Therefore, it is useful to consider what incentives businesses have to share their data. In particular, the incentive to share data may vary depending on the purpose for which a business is requesting it. For example, if the data is being requested to develop a competing good or service, then the business may be less inclined to share it.[49]

There are a number of possible *market failures* associated with the collection and use of consumer data including i) asymmetric information; ii) externalities; and iii) a possible lack of competition. *Asymmetric information* can occur where there is an imbalance in information between buyers and sellers, which can potentially lead to inefficient market

[47] *Supra* note 41 at 17-18.
[48] *Id.*
[49] *Id.* at 21.

outcomes. [50] The existence of externalities may mean that consumer data are collected and traded at sub-optimal levels in terms of maximising welfare. Other academics have argued that a lack of privacy protection in certain markets may be the result of *market power* in those markets.

This means that consumer data is increasingly relevant to competition assessments. [51] This can manifest in two key ways: i) privacy and data protection might be an aspect of quality on which businesses may compete; ii) the collection and ownership of consumer data, and access to that information, might impact competition.[52]

Market failures within platforms are not only the "classic" ones that act on the supply side and market structure, but also those, more recently studied in behavioral economics (framing, prominence, self-confirmation bias, default bias, etc.), which concern demand dynamics. One issue is that privacy trade-offs are intertemporal in that sharing data will likely bring an immediate (and more certain) benefit, as compared to the risks of an uncertain cost at some unknown future date. In addition, consumers may underappreciate privacy in zero-price markets (and over-appreciate the benefits of the free good or service) due to the "free effect". [53] Commentators have also raised concerns about consumers' lack of bargaining power in respect of privacy notices, which tend to be provided on a "take it or leave it" basis. These issues can manifest in the so-called "privacy paradox", where, despite expressing concerns about privacy, and rating it as important, consumers do not appear to make decisions with privacy in mind. [54]

Given the pervasiveness of the datafication phenomenon in the economy, it becomes particularly urgent in some areas to consider Big Data in the economic analyses conducted to understand the competitive process, including within the competencies of competition authorities.[55] Business models based on Big Data constitute a deeply

[50] In particular, if consumers cannot verify information before making a purchase, this can lead to an "adverse selection" or "lemons" problem, where higher quality goods (e.g. more privacy protective goods and services) are driven out of the market
[51] *Supra* note 41 at 23-25.
[52] *Id.*
[53] *Supra* note 23, at 29.
[54] *Id.*, at 94-95.
[55] *Id.*, at 71-75.

distinguishing aspect of digital ecosystems and services, characterized by high levels of concentration and the presence of operators holding dominant positions.

In markets where the use of Big Data assumes particular importance in service provision and, therefore, in the competitive process, availability of Big Data can contribute cumulatively to the high degree of concentration and the existence of barriers to entry in digital markets, arising from other factors such as network externalities. [56]

The utilization of big data becomes notably relevant in instances where online platforms give rise to multi-sided attention markets (such as online search engines or social networks) or exchange markets (e.g., e-commerce marketplaces). [57]

More data allows for greater value generation for advertisers, increasing revenues that can, in turn, be invested in service quality, leading to indirect network effects. These network effects can progressively lead the entire market to favor a particular platform (market tipping), consolidating its position. [58]

In order to understand whether and to what extent the combination of Big Data and network effects allows first movers to benefit from a competitive advantage over potential new entrants, the issue needs to be addressed with reference to a specific market, considering three aspects: i) the relevance of Big Data for providing the good/service in light of all the characteristics of the market in question; ii) the nature, quality, and quantity of data required to compete effectively; iii) the number/variety of sources (both online and offline) that can be used to generate the relevant knowledge to offer the services competitively.[59]

In order to encourage exploration by consumers and to allow entrant platforms to attract them through the offer of targeted services, it is key to ensure that multi-homing and switching are possible and dominant platforms do not impede it.[60]

The significance of data and data access for competition will always depend on an analysis of the specificities of a given market, the type of data, and data usage in a given case. The GDPR can facilitate the switching between data driven services, through data

[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] Supra note 3, at 6

portability (article 20).[61] More demanding regimes of data access, including data interoperability, can be imposed (i) by way of sector-specific regulation (as in the context of the Payment Services Directive 2015/2366/EU) – in particular where data access is meant to open up secondary markets for complementary services; or (ii) under Article 102 TFEU – but then confined to dominant firms. [62] Where competitors request access to data from a dominant firm, a thorough analysis will be required as to whether such access is truly indispensable. In addition, the legitimate interests of both parties need to be considered. It is necessary to distinguish between different forms of data, levels of data access, and data uses. In a number of settings, data access will not be indispensable to compete, and public authorities should then refrain from intervention. There are other settings, however, where duties to ensure data access – and possibly data interoperability – may need to be imposed. This would be the case, in particular, of data requests for the purpose of serving complementary markets or aftermarkets – i.e. markets that are part of the broader ecosystem served by the data controller.[63]

2.3) Platforms and ecosystems: the business model of Tech Giants

While in other industries reducing costs can be a major source of competitive advantage, this is often less the case in the digital world. [64] Competition among platforms primarily revolves around the dimension of product and service innovation, whose benefits are achieved by being "first to the market" and developing a large user base. [65] Innovation fostered by competition between platforms has improved the welfare of consumers by improving their interconnectivity, giving them access to new marketplaces and new services and enabling the efficient and very cheap distribution of cultural content. Moreover, it has bolstered the efficiency of firms by allowing large amounts of data to be collected, shared, and used across supply chains.

In the digital economy, innovation-driven competition transcends individual platforms, encompassing entire *ecosystems* - ensembles of services, some complementary,

[61] GDPR, *supra* note 38, art.20.
[62] *Supra* note 3, at 8-10.
[63] *Id.*
[64] *Id.* at 32.
[65] *Id.* at 35.

interconnected through private APIs, and thus accessible only to services from the same ecosystem. If such privileged access to a user's data or connectivity with other services or Internet of Things devices allows a service from the ecosystem to offer a much better product, competitors will not be able to compete on the merit. Devices belonging to different ecosystems are harder and sometimes impossible to use together. Similarly, services from the ecosystem are often pre-integrated with one another, including data interoperability. This has several implications for competition, including lock-in into an ecosystem, data concentration and the difficulty for complementary services to develop and compete on the merit. [66]

Additionally, large multiservice platforms benefit from *"economies of scope":* once they offer one service, they become more efficient at offering others. Economies of scope can arise from network externalities, leveraging an existing and trusting user base and thereby addressing the challenge of starting a service with robust network effects. Alternatively, economies of scope could result from the redeployment of technology that has proved fruitful in other areas. [67]

All of these elements are by themselves pro-competitive: if large incumbent ecosystems are better at offering new services, there might be advantages in allowing them to do so. However, this might also prevent competition on the merits for new services. Given the stickiness of market power, enhanced by the specificities of competition in the digital market, there is legitimate fear that new entrants will potentially face difficulties in trying to challenge a platform's entrenched market dominance. [68] With network externalities and increasing returns to scale, economic theory predicts that there can be only a few platforms competing to provide any given type of service. If this is the case, competition *"in"* the market will be limited. Instead, the emphasis shifts to competition "for" the market—competition to enter and potentially replace a platform that holds a dominant position in providing a particular service.[69]

Some argue that this competition is extremely intense and that, therefore, incumbent firms have limited possibilities to exploit their market power, as they attempt to fend off

[66] *Id.*
[67] *Id.*
[68] *Id.* at 70.
[69] *Id.* at 36-38.

competitors who try to take the whole market from them. [70] However, in markets where network externalities and returns to scale are strong, there is, without multi-homing, protocol and data interoperability or differentiation, place for only a limited number of platforms. In essence, the success of any attempt to challenge an incumbent will depend on the ability of a potential rival to attract a critical mass of users and generate its own positive network effects. Actions by a dominant platform that hinder rivals from doing so, or raise their costs, without constituting "competition on the merits", should therefore be suspect under competition law. [71]

Over the past 15 years, scholars and practitioners have extensively explored the challenges that platforms pose for competition policy, particularly focusing on the implications of network externalities for market definition and enforcement.[72] More recently, scholars have turned their attention to the fact that a special feature of the intermediation function that platforms frequently fulfill is that it is accompanied by a rule-setting function: many platforms, in particular marketplaces, act as *regulators,* setting up the "rules and institutions" through which their users interact. [73] Rule-setting by platforms will take on different forms, depending on their function and design. For example, the "regulatory" function of a search engine will largely align with the design of the ranking algorithm, hence with its core service. Furthermore, because of this function as regulators, the operators of dominant platforms have a responsibility to ensure that the rules that they choose do not impede free, undistorted and vigorous competition, and that the latter is instead fair, unbiased, and pro-users. [74] The rules and institutions established by a dominant platform must not anti-competitively exclude or discriminate. When a dominant platform operates a marketplace, it must ensure a level playing field and refrain from using its rule-setting power to influence competition outcomes. [75] When competitive pressure is sufficient, platforms lack incentives to

---

[70] This view is somewhat akin to the "contestable market" theory of the 1980s and 1990s, which argued that markets with very few firms could still be considered competitive because of the presence of potential entrants.

[71] *Supra* note 3 at 36-38.

[72] *Id.* at 60-63.

[73] *Id.*

[74] *Id.*

[75] *Id.*

reduce competition or offer goods that do not meet consumer requirements. However, network externalities and information asymmetries often reduce competition intensity, making such practices profitable without intervention by competition authorities.[76]

Viewing marketplace platforms as regulators highlights a problematic scenario that arises when the platform or another service from the same ecosystem is also a participant in the market. [77] This raises concerns about how platforms treat their own products and services compared to those provided by other entities. Giving preferential treatment to one's own products or services, or one from the same ecosystem, when they are in competition with products and services provided by other entities, constitutes a specific technique for leveraging a platform's market power, namely, *self-preferencing*. [78] In cases of vertically integrated dominant digital platforms in markets with particularly high barriers to entry, and where the platform serves as an intermediation infrastructure of particular relevance, to the extent that the platform performs a regulatory function, it should bear the burden of proving that self-preferencing has no long-run exclusionary effects on product markets. [79]

Despite the large availability of data and real-time market information, providing many opportunities for pro-competitive exchanges of data, it is often the case that vertically integrated platforms guarantee privileged data access to their own subsidiaries. [80] Therefore, the interpretation of the GDPR by a handful of large operators arguably plays a significant role in shaping competition within an industry. As observed by the CMA: "The changes that can potentially have the largest impact on competition among intermediaries will result from providers' interpretation of what privacy protection requires, rather than from direct enforcement of data protection regulations. Decisions made by the largest market participants, Google above all, will have the greatest impact on the industry."[81] Google is the leading provider of ad tech services across virtually

[76] *Id.*
[77] *Id.,* at 65-70.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] Competition and Markets Authority, Market study final report, Appendix M: intermediation in open display advertising, 1 July 2020, available at https://assets.publishing.service.gov.uk/media/5efb22add3bf7f769c84e016/Appendix_M_-

every step of the value chain between marketers and publishers, hence its policy decisions affect the ecosystem at large. However, Google also happens to operate Chrome, the most popular browser (with an estimated market share of about 66% on a worldwide basis) and Android, which runs on more than 70% of all smart mobile devices.

Apple, on its part, operates the second most popular browser (Safari; estimated worldwide market share of 17%), while its iOS operating system runs on approximately 26% of all smart mobile devices. [82] In order to identify users, a company relies from a technical point of view on the user's browser (with respect to cookie-based identification) and/or the user's smart mobile OS (with respect to identification based on mobile device advertising identifiers). This technological dependence, in turn, means that the companies controlling the most popular browsers and smart mobile OSs – Google and Apple – have unique power over all ecosystem participants.

Consequently, the policy decisions of these companies can shape the rules of engagement for all ecosystem participants, including how they identify users in web and app environments.[83] Since many such policy decisions are said to be motivated by privacy and data protection considerations, it is often referred to these companies as "*de facto* privacy regulators."

Importantly, these *de facto* privacy regulators typically go beyond what is required to ensure compliance with any privacy law, and often impose on ecosystem participants their own view on how compliance is to be achieved, even if the legislation in question affords operators with discretion over the exact way of compliance.

In the context of online advertising, Google and Apple get to decide the "right" trade-off between privacy, competition and efficiency, and impose their value judgment on all ecosystem participants. In the second place, to the extent the policy changes of the de facto privacy regulators limit the ability to identify users, one may argue that they result in a welfare gain for users, e.g., in the form of enhanced privacy, which may be considered an increase in service quality. But this gain would have to be weighed

_intermediation_in_open_display_advertising.pdf ("CMA Final Report, Appendix M: intermediation in open display advertising"), paragraph 539.

[82] *Supra* note 11, at 33-37.

[83] *Id.*

against the welfare losses resulting from any limitations in the ability to perform legitimate advertising use cases (e.g., ad personalization, conversion measurement and attribution). Such limitations imply a welfare loss for publishers, marketers and users. [84] This raises competition concerns, similar to those raised with respect to platforms holding a "dual" role, such as being the marketplace and competing in the marketplace.

3. Theoretical framework for the analysis of abuse of dominance cases in a Data-Driven Economy

3.1) Article 102 of the Treaty of the functioning of the European Union

Competition law concerns the behaviour of companies and abuse of market power. Its primary objectives revolve around bolstering the efficiency of the internal market and safeguarding the welfare and options accessible to consumers. [85] Consumer welfare has not been defined in EU law and its relationship with market efficiency is not commonly understood.[86] As recognized by the Commission in its "guidelines on enforcement of rules on abuse of dominance"[87], welfare is determined not only by price, but also by other factors, such as quality and consumer choice, which is also a relevant concern for data protection.[88] Scholars have posited that the fundamental aim of competition law is to guarantee that the internal market adequately meets consumers' reasonable wishes for competition. This encompasses not only the wish for competitive pricing but also the wish for diversity, innovation, quality, and other non-price benefits, including privacy protection. [89]

[84] As pointed out by the CMA, "Measures which enhance an aspect of consumer privacy in the near term,may have dynamic effects which risk a negative impact on consumer welfare, for example a concentration of personal data amongst fewer providers, so impacting consumer choices and control in the longer term". *See* CMA Online Platforms and Digital Advertising Market Study(July 1, 2020), paragraph 5.328, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.
[85] *Supra* note 10 at 16-21
[86] Economists generally understand consumer welfare as the individual's own assessment of his/her satisfaction with benefits derived from the consumption of goods and services as compared with prices and income. Exact measurement of consumer welfare therefore requires information about individual preferences; *see*, for example, OECD Glossary of Industrial Organisation Economics and Competition Law.
[87] Article 19 of Commission Guidance 2009/C 45/02.
[88] *Supra* note 10 at 16-21
[89] *Id.*

The European Commission Treaty on the Functioning of the European Union (TFEU) Preamble includes acknowledgement that action is required to achieve, among other things "fair competition."[90] Though not exclusive to competition law, economic policy provisions of TFEU specify that Member States and the Union shall act "in accordance with the principle of an open market economy with free competition, favoring an efficient allocation of resources..."[91] and "in accordance with the principle of an open market economy with free competition."[92]

To these ends, Articles 101-102 TFEU prohibit agreements between companies which would prevent or distort competition, seek to prevent abuse of a dominant position, and require the Commission to investigate cases of suspected infringement of the principles of competition.[93] Enforcement of EU competition rules, often involves an assessment of the market power of a given undertaking and of whether the latter occupies a dominant position. [94] Before analyzing whether a certain conduct from an undertaking is abusive, it is therefore necessary to first establish dominance in the relevant market on which the undertaking is active. [95]

The Commission evaluates market power and market structure through an assessment of market share, that is, the relative importance of the various undertakings active on the market. The usual determinant in the assessment of market share is company turnover, or volume or value of total sales of the relevant product in the relevant area. [96] Market share is then interpreted in the light of the specific conditions of the market: for measuring market share in one specific sector relevant to the digital economy, Commission guidelines recommend the selection of whichever criteria are most appropriate in the light of the characteristics of the market. Market dominance becomes

[90] Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47, at Preamble [*hereinafter* TFEU]
[91] *Id*. at Art.120
[92] Id. at Art. 119
[93] *Supra* note 10 at 16-21
[94] *Id.*
[95] Reverdin, Vladya M K. "Abuse of Dominance in Digital Markets: Can Amazon's Collection and Use of Third-Party Sellers' Data Constitute an Abuse of a Dominant Position Under the Legal Standards Developed by the European Courts for Article 102 TFEU?" *Journal of European competition law & practice* 12, no. 3 (2021): 181–199.
[96] *Supra* note 10 at 16-21

likely, though not inevitable, where an undertaking's market share equals or exceeds 40%.[97] The Commission also considers barriers to expansion or entry into the relevant market, listing as examples economies of scale, privileged access to essential inputs, and costs or other impediments to customers switching to new suppliers.[98]

Case law has established that a dominant undertaking has a 'special responsibility' not to conduct itself in such a way that harms competition: it may seek to protect its own interests under attack from competitors but not to strengthen its dominant position. [99] Dominance, in competition terms, involves the ability to determine prices and to control production in a given market. Dominance in a relevant market does not in itself constitute an infringement of competition rules. However, the abuse of a dominant market position which "affects trade between Member States"[100] is prohibited under Article 102 TFEU. [101] Such abuse has tended to be understood as taking one of two forms: i. exclusionary conduct, where a dominant undertaking excludes actual or potential competitors by means other than competing on the merits of the products or services they provide; and ii. exploitation, or action which 'directly' harms consumers through, for example, charging excessively high price.

The Commission has issued enforcement guidance in relation to exclusionary conduct by dominant undertakings. Exclusionary conduct is abusive where it results in 'foreclosing (the dominant undertaking's) competitors in an anti-competitive way', therefore potentially damaging the competitive market structure. [102] The Commission's guidance identifies specific forms of exclusionary conduct, namely, *exclusive dealing*, *tying and bundling*, *predation* and *refusal to supply* and *market squeeze*. Such actions are deemed to be most harmful to consumers and to have adverse impact on consumer welfare. [103] One form of exclusionary conduct, refusal to supply, contains the concept of an'essential facility','a product or service that is objectively necessary to be able to

---

[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] Commission Notice Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, 2004/C 101/07.
[101] *Id.*
[102] Article 19 of Commission guidance 2009/C 45/02.
[103] *Id.*

compete effectively' and for which there is no alternative product or service and where technical, legal or economic obstacles make it impossible or unreasonably difficult to develop an alternative.[104] Refusal to supply such a facility is likely to lead to elimination of effective competition or to consumer harm. [105]

3.2) Analytical challenges for Antitrust Authorities

The challenges stemming from the rise of the Internet, the 'new economy' and the digital economy necessitate a reevaluation of how the foundational framework of competition law, as outlined in Articles 101 and 102 of the TFEU, is implemented. The unique characteristics of platforms, digital ecosystems, and the data economy call for adjustments and enhancements to established concepts, doctrines, methodologies, and the enforcement of competition law itself.[106]

The first stage in the legal analysis of cases of anti-competitive agreements, mergers and abuse of dominant market position is the definition of the relevant antitrust markets and, subsequently, the evaluation of the firm's market power, defined as the ability to raise prices above those that would be charged in a competitive market, or the similar ability to reduce quality or output below competitive levels while sustaining profitable sales volumes.[107]

The definition of the relevant market allows competition regulators to identify the market operators, that is, suppliers, customers and consumers, and to calculate the total market size and the market share of each supplier with reference to the relevant product or service in the relevant area. This exercise in general considers three variables:

a) the product market, including products and services which are considered by consumers to be interchangeable or substitutable; this consideration includes

---

[104] The essential facilities doctrine originated in US case law and states that owners of essential facilities are obliged to deal (the 'obligation to supply') with competitors. It has not been explicitly cited by CJEU, but in C- 7/97 Bronner v Mediaprint Zeitungs [1998], the court restricted the obligation to supply to situations in which the owner of an indispensable facility held more than a dominant position.

[105] *Supra* note 10 at 16-21.

[106] *Supra* note 3 at 39-40.

[107] Erika M. Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy,* Annex 2 to the Report To The Global Privacy Assembly Digital Citizen and Consumer Working Group, (July 2021).

supply side substitutability, that is, the possibility of switching on the production side;

b) the geographic market, the area where generally similar competition conditions prevail which are distinct from neighbouring areas; and
c) a time horizon, reflecting the changes in consumer habits and technological developments [108]

While acknowledging that digital markets may pose specific analytical challenges, antitrust agencies have tended to reaffirm the resiliency, flexibility and applicability of existing analytical frameworks for market definition. Within these existing frameworks, though, antitrust enforcers recognize that digital markets often exhibit specific features that impact and add complexity to antitrust analysis, such as prevalent network effects and the heightened importance of non-price competition.[109]

For example, consider the common analytical tool used to assess substitutability and define markets, particularly in modern merger review- namely, the hypothetical monopolist paradigm. As mentioned above, there is a limit to the ability of firms to increase prices in zero-price markets, meaning that a SSNIP test is likely not to be of value for market definition. [110]There may be a heightened risk, therefore, of "injecting subjectivity into the process of market definition". [111]

For products or services in zero-price markets, multiple jurisdictions have posited that, instead of focusing on the effects of a price increase, in defining relevant markets, antitrust analysis might use a small but significant non-transitory decrease in quality (SSNDQ) test. [112]Discussion of the SSNDQ analysis tends to acknowledge that it will be more difficult to operationalize such a quality-based test than it is the standard, price-based approach. This analysis is further complicated by the two-sided nature of many digital markets, where one group (often the end consumers) receives the products free of charge, while another group pays a monetary price that subsidizes the non-paying

[108] *Supra* note 10, at page 18.
[109] *Supra* note 108, at 75.
[110] *Id.*
[111] OECD, Directorate for Fin. & Enter. Affairs Competition Comm., *Quality Considerations in Digital Zero-Price Markets – Background Note by the Secretariat*, at 31 (Nov. 28, 2018), https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf
[112] *Supra* note 108, at 76.

side. Cross-side effects in such markets can add complexity to the valuation of changes in service quality. In practice, however, the difficulties of using the SSNIP test or the SSNDQ test have not been an obstacle to market definition in EU antitrust and merger cases concerning platforms in general, and zero-price services in particular, as the Commission has instead turned to assessing service functionalities, as a means to assess demand substitutability. [113]

Another important aspect, adding complexity to the definition of relevant markets, needs to be taken into account: when studying issues associated with multi-sided platforms, competition policy must analyze all the sides and consider all their interactions. In most cases, different markets are defined on both sides. In the case of platforms, the interdependence of the markets becomes a crucial part of the analysis, whereas the role of market definition traditionally has been to isolate problems. Therefore, in digital markets, less emphasis should be put on the market definition part of the analysis, and more importance attributed to the theories of harm and identification of anti-competitive strategies.[114]

The second crucial step in antitrust analysis, as previously mentioned, is the evaluation of market power, used to identify cases of market dominance. Traditionally, market power has been measured by market shares, i.e. by the ratio of sales of a firm to the total sales in the market, and market dominance has been assumed when the market share was above a certain threshold. However, commentators have highlighted how, in the presence of network effects, prices do not necessarily represent the value of the good or service to the consumers or to the firms which are selling them, hence the percentage of sales does not make much sense.[115] This is obviously true when the price is equal to zero, but is also true in other two- sided markets. Therefore, the concept of market share is often not a useful tool to measure market power.

---

[113] *Supra* note 3, at 45.
[114] *Id.*, at 46.
[115] Supra note 3, at 43; when prices represent the social value of goods, they can be used to compute the variations of consumer welfare induced by different policies. This is not the case for services for which there are network externalities. Because one cannot read directly from the prices the total consumer value of the last unit purchased, computing variations of consumer welfare becomes much more difficult

In the case of platforms, increasing returns to scale, network externalities and data – further reinforce the difficulty of measuring market power. [116] In this regard, it has been previously mentioned how accumulation of data may act as a barrier to competition.[117] Antitrust agencies have considered the potential for data accumulation, and data use, to create barriers to entry and expansion to enhance market power. Where a firm accumulates data that is unique and difficult for competitors to replicate in scale or type, that data may create challenges for competitive entry and contribute to market power.[118] Furthermore, often, demand side distortions like information asymmetries and consumer biases, arising out of the specificities of digital markets, contribute to enhance the market power of incumbents, who exploit them in the attempt to marginalize rivals and reduce competition. [119] Therefore, any examination of market power should meticulously evaluate, on a case-by-case basis, the preferential access to data available to the presumed dominant firm, the sustainability of such differential data access, and take into account demand-side distortions.[120]

As pointed out by some scholars, however, neither market definition nor market power analysis have expressly focused on privacy. [121] Instead, antitrust authorities have looked at the broader considerations posed by digital markets, including the challenges of zero-price products and the role of data in competition. Since price cannot form the basis for competition in zero-price markets, *privacy* and other aspects of *product quality* may take on a more prominent role in competition in these same markets.

[116] I*d.,* at 49
[117] *See*, Section 2.3.
[118] *Supra* note 108, at 79.
[119] *Supra* note 3, at 50.
[120] I*d.*
[121] *Supra* note 108, at 75.

3.3) Integrating Data privacy into Antitrust analysis: the "privacy as quality" theory

The predominant theory regarding the intersection of antitrust law and data privacy suggests that antitrust analysis should incorporate privacy considerations when privacy serves as a component of product or service quality impacted by competition. This perspective, often referred to as the "privacy-as-quality" view, represents the most extensively discussed and developed theory concerning the connection between data privacy and potential antitrust harm. However, a thorough understanding of the theory's complete significance, implications, and potential applications is still in its nascent stages. Data privacy authorities have endorsed a similar perspective, viewing privacy as a component of product quality and competition. [122] For instance, the European Commission's two-year retrospective on the GDPR notes that "many businesses also promote respect for personal data as a competitive differentiator and a selling point on the global marketplace, by offering innovative products and services with novel privacy or data security solutions." [123] Additionally, privacy agencies frequently cite research indicating that consumers increasingly prioritize privacy when making product choices.

However, it is worth noting that the OECD characterizes the privacy-as-quality viewpoint as "the subject of debate" due to perceived limitations on consumers' ability to assess privacy quality as part of their decision-making process. [124]In particular, factors such as information asymmetries and other distortions may render consumers unable or unwilling to accurately evaluate the true privacy quality of products and services. The result may be sub-optimal privacy competition—less consumer demand for privacy controls leads to reduced competition among firms to provide these controls,[125] such that competition alone cannot be relied upon to drive optimal levels of privacy.

---

[122] *Id.* at 62-71.

[123] Eur. Comm'n, *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*, at 3 (June 24, 2020), https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN;

[124] OECD, Zero-Price Markets – Background Note, *supra* note 112, at 7

[125] *Id.*

As it is currently understood, this privacy-as-quality theory plays both an integrating and a limiting role at the intersection of privacy and antitrust law. The theory incorporates data privacy into longstanding antitrust analytical frameworks, which recognize that quality can serve as a basis for competition in markets.[126] This integration hinges on interpreting "quality" expansively enough to encompass competition based on privacy features or offerings. Where the law and agency guidance enable antitrust to account for non-price competition more generally, it opens the door to consideration of the quality of data privacy. This retention of the core principle of consumer welfare, albeit broadly construed, may explain the increasing recognition and acceptance of the privacy-as-quality theory. It offers a means of accounting for data privacy in a manner that does not require a substantial rethinking of the fundamental tenets of antitrust law.[127] At the same time, multiple antitrust agencies view the privacy-as-quality theory as circumscribing their jurisdictional scope in addressing privacy concerns. In other words, standalone privacy concerns with no nexus to competition are not considered cognizable in antitrust law. Such pure privacy harms, divorced from any competitive context, are typically seen as falling within the domain of privacy law and agencies. This stands in contrast to privacy-as-quality effects that intersect with competition and which may be factored into antitrust analysis.[128] The major concern with taking a broader view of how privacy relates to antitrust—such as a view that uses antitrust law to police privacy harms unrelated to competition—is that it will dilute and confuse antitrust law doctrine. Such an approach would introduce privacy considerations, which often encompass broad, non-economic, and potentially subjective or normative aspects, into antitrust analysis that traditionally focuses on economic consumer welfare, efficiency, and competition.[129]

Despite the growing theoretical recognition that privacy may be an element of competition, assessing privacy-related competitive effects is likely to present practical challenges. Antitrust analysis at all stages is permeated by price-based tools and methodology. Price effects serve as a fundamental cornerstone of antitrust law and the economic models underpinning it. From market definition and market power analysis,

---

[126] *Supra* note 108, at 62-71.
[127] *Id.*
[128] *Id.*
[129] *Id.*

to measurement of the competitive effects of conduct and mergers, price is the primary touchstone for antitrust analysis and modeling. [130] Measuring non-price effects has long posed a challenge for antitrust law, and the analysis of privacy quality is merely the latest manifestation of this broader issue. Indeed, price-based analysis is so fundamental to antitrust law that arguments continue to be made that antitrust doctrine is inapplicable to markets where consumers do not pay a monetary price for products or services. [131] The question of antitrust law applicability to "zero-price" markets is therefore also of relevance to privacy-based competition. The primary obstacle lies in the absence of established analytical approaches for antitrust to evaluate changes in the magnitude or quality of privacy protection concerning misconduct or mergers. Assessing privacy quality and the impact on consumers of declining quality may prove challenging for several reasons.

As aknowledged in privacy literature and by regulatory agencies, consumers often exhibit *heterogeneous privacy preferences*.[132] Some consumers may perceive additional personal data processing as advantageous if it enables them to access a new service or feature, or if it allows them to use a service without charge. Conversely, others may view such practices as a reduction in quality and prefer to pay for a service that does not collect their personal information. The complexity of assessing competitive effects is further compounded by the trade-off between the detriment to privacy quality and potential improvements in other aspects of product quality. Additionally, measuring privacy quality may be hindered by documented distortions in consumer preferences regarding privacy choices. [133]As the OECD observes, many of the analytical tools developed for market definition and assessment of competitive effects were created to measure price impacts, and therefore "alternative tools are needed to assess demand (and supply) substitutability in respect of quality." [134] The OECD proposes that in zero-price markets, indicators such as "measures of online user attention, transaction volume, and evaluations of network effects and the prevalence of multi-homing" could prove

[130] *Id.*
[131] *Id.*
[132] OECD, Zero-Price Markets – Background Note, *supra* note 112, at 10
[133] *Id.*
[134] OECD, Directorate for Fin. & Enter. Affairs Competition Comm., *Executive Summary of the Discussion on Quality Considerations in the Zero-Price Economy* - Annex to the Summary Record of the 130th Meeting of the Competition Committee held on 27-28 November 2018, at 5 (2018), https://one.oecd.org/document/DAF/COMP/M(2018)2/ANN9/FINAL/en/pdf

valuable in competition assessment. [135]

Another potential approach to analyzing privacy effects is to estimate the monetary value of the data being provided by consumers. In this perspective, often referred to as "data as currency theory", consumers "pay" for services with their data, and the antitrust analysis endeavors to quantify the value of the value of data collection, usage, or other processing in terms of prices. [136] For zero-priced services and markets, this approach integrates non-price analysis into antitrust, price-based models. For other digital products and services, the existing business models may provide insight into the monetary value consumers assign to their data or privacy. For instance, consumers may pay an additional fee for privacy-protective features or opt for a version of a service without behavioral advertising, even if a free, ad-based version is available.[137] Some skepticism has been expressed regarding antitrust analyses that translate data privacy or processing into monetary terms. While equating data processing with a monetary value might seem expedient for antitrust purposes, it could pose challenges in jurisdictions where data privacy is considered a fundamental right. Furthermore, the determination of the monetary value consumers place on privacy or data processing is still likely to face challenges in accounting for consumer biases, and the tradeoffs between data disclosure and other facets of product or service quality. [138] The OECD concludes that, instead of equating data to currency, analysis akin to that of "any other dimension of quality remains the most practical approach."[139]

[135] *Id.*
[136] *Supra* note 108, at 62-71
[137] *Id.*
[138] *Id.*
[139] OECD, Zero-Price Markets – Background Note, supra note 112, at 15.

3.4) Privacy considerations in abuse of dominance: focus on Self-Preferencing

There is not yet a concrete understanding of the relationship, causal or otherwise between monopoly and data privacy or privacy law, and a few abuse of dominance cases have expressly considered privacy. [140]

The result is that interactions at the juncture between abuse of dominance and data privacy are at a very early stage of development. When antitrust agencies refer to the connection between monopolization and privacy, it tends to be in portraying market power, or a lack of competition, as a likely cause of low privacy quality or choice for consumers. Low privacy quality has been portrayed by some antitrust authorities as a symptom of abuse of dominance in markets where companies consistently infringe privacy rules without facing competitive constraints in response.

On the other hand, data privacy regulators have observed that enforcing prohibitions against abuse of dominance could foster the development of privacy-enhancing services within affected markets. Following this reasoning, increased competition could be expected to improve the standard of privacy protection in markets where privacy-oriented features or products are a key element of competition.[141]

The reality may prove more intricate, given the acknowledged challenges consumers encounter when making privacy choices and the potential impacts on privacy-related competition. Determining whether and when competition or monopoly is likely to result in greater privacy benefits for consumers, is a significant question worthy of consideration by both privacy and antitrust authorities. [142]

Several antitrust agencies acknowledge another possible relationship between privacy and monopoly: privacy laws that are difficult to comply with may contribute to the entrenchment of existing monopolists. However, while abuse of dominance is premised on market power, the application of data privacy law is not explicitly contingent on the

[140] *Supra* note 108 at 99-106.
[141] *Id.*
[142] *Id.*

enterprise's position in the market; in other words, privacy obligations apply to all entities, irrespective of their size or dominance. [143]

Moreover, another facet of the relationship between abuse of dominance and privacy is the power and control that large digital companies exert over online environments, which has raised concerns among both privacy and competition authorities. By virtue of their central position in the digital ecosystem, many dominant firms develop the rules and act as the arbiters for permissible and prohibited conduct on, and access to, popular websites and other platforms. [144]

For instance, Google regulates the content displayed in online search results and search advertising on its widely-used search engine, while Apple controls access to its app store, where both Apple and third parties offer applications for mobile devices. Each company establishes and enforces the terms and conditions of access to their digital commerce sites, dictating who and what is permitted on these major platforms. Several antitrust agencies refer to this as the online "gatekeeper" function of digital platforms, although the term lacks a settled or legal definition. [145] It has become commonly employed to denote the quasi-regulatory role digital platforms often assume in controlling access to popular online competition sites. For both antitrust and data privacy, the influence that platforms wield over digital ecosystems typically serves as a general policy consideration or starting point for analysis rather than constituting a violation of either area of law in itself.

In most jurisdictions, acting as a gatekeeper is not a violation of antitrust law. At the EU level, there is also new legislation specific to digital markets that will create regulatory obligations (beyond that of antitrust or privacy law) that are imposed on large digital platforms.[146]

This policy concern surrounding the power of digital platforms, also prompts inquiries into the equilibrium between competition and data privacy in digital environments. Faced with increasing privacy compliance obligations, numerous large platforms have

[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] EDPS, Opinion 2/2021, Digital Markets Act (Feb. 10, 2021); EDPS, Opinion 1/2021, Digital Services Act (Feb. 10, 2021).

pursued high-profile transitions toward *walled garden* business models, enhancing their control over consumer data and enclosing that data within their technological ecosystems. [147] With the rise of the digital economy and its many data-driven business models like Google and Apple's, data-related theories of abuse of dominance have seen renewed antitrust attention. Data accumulation in itself is not inherently abusive and can even enhance product and service improvements, fostering the competition that antitrust laws aim to protect. Therefore, it is specific conduct associated with data use, rather than the mere collection and holding of data, that may trigger antitrust concerns. In addition, to violate antitrust law, the conduct must have a sufficiently negative effect on competition.

Multiple jurisdictions have considered different data-related theories of *exclusionary conduct*: (i) exclusion of rivals from important sources of data collection, through the use of exclusivity agreements with buyers or suppliers, (ii) bundling or tying of products or services that buyers would not otherwise purchase together, in a manner that reduces competition, (iii) leveraging of a monopoly from one market where the dominant firm has market power into an adjacent market. [148] Finally, some jurisdictions have raised the possibility that certain data could constitute an "essential facility" to which rivals require access to compete.[149] Since data, by its nature, is generally a *non-rivalrous* resource, an important question in such cases is whether the rival could replicate the data itself in order to compete, rather than relying on access to the dominant firm's data set. Thus, the role of data in a particular market would need to be examined on a case-by- case basis. A fundamental, and often difficult, question will be whether the data- related effects are the result of product improvement on the merits—which antitrust law encourages—or instead constitute an abuse of market power, which antitrust law prohibits.[150]

---

[147] *See* discussion in-text of Google third-party cookies termination; Thornhill, John." Apple's Move To Increase Privacy Strengthens Its Walled Garden*." Financial Times* (March 18, 2021), (discussing Apple's new operating system which will present users with more options to control in-app tracking).

[148] *Supra* note 108 at 99-106.
[149] *Id.*
[150] *Id.*

Several agencies have expressed concern that competition will suffer where large digital platforms use their "gatekeeper" status to self- preference, discriminating in favour of their first-party services, by "making third party services or products less prominent, ranking them lower, degrading or delaying their access to the platform, or worsening their terms and conditions of access." [151]The two cases examined in the subsequent sections of this study, *Apple ATT* and *Google Sandbox*, involve vertically integrated platforms, acting as gatekeeper and engaging in exclusionary conduct by imposing stricter data collection conditions on their competitors than those imposed on their own first-party services. The allegation is that this dual role as both "gatekeepers" or operators of the sites where online competition occurs and competitors to third-parties who rely on access to the gatekeeper-controlled sites, is being used to engage in anticompetitive conduct. Article 102 TFEU does not impose a general prohibition of self-preferencing on dominant firms. [152] In other words, self-preferencing is not abusive *per se*, but it may constitute an abuse of dominance when the conduct involves the previouly mentioned forms of exclusionary conduct by a dominant firm such as monopoly leveraging or refusals to deal. Moreover, it is best understood as a specific variation on broader and more established theories of competitive foreclosure or exclusion.[153]

In the past years, beliefs that platforms providing differentiated treatments by favouring their own activities can produce anticompetitive effects have significantly increased. [154] In 2017, the Commission fined Google for treating its comparison shopping service more favourably by increasing the visibility and placement of its service.[155] The decision raised numerous debates, particularly due to the uncertain theory of harm, which the Commission relied upon. In particular, European Union (EU) competition law does not require dominant undertakings to ensure the survival of their competitors in the market, and harmful conducts are not prohibited unless competition is affected through particular exclusionary behaviours such as tying or refusal to deal. However,

[151] *Supra* note 2, at 1-2.
[152] *Supra* note 3, at 7.
[153] *Supra* note 108, at 113.
[154] *Supra* note 96, at 182-184.
[155] Summary of Commission Decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39740 – Google Search (Shopping)).

the 2017 decision of the Commission in Google Shopping, advocates that self-preferencing in itself *can* be abusive, in particular when it enables the undertaking to leverage its dominant position from upstream to downstream markets. By framing the decision as one of leveraging and self-preferencing, the Commission bypassed the stricter conditions of the Essential Facility Doctrine, but failed to lay down the legal test against which the lawfulness of these conducts should be assessed. [156]

Therefore, it remains difficult to grasp which legal test is relevant to assess the lawfulness of leveraging and self-preferencing and whether indispensability of data is a condition to establish an abuse, as the criterion was not applied to Google's general search results pages. If favouring and discriminating are in themselves problematic, this would entail that vertically integrated dominant firms would never be allowed to refuse to give access to their input.

The report 'Competition policy for the digital era', drafted for the Commission, acknowledged that self-preferencing can result in an abuse not only under the EFD, but also when it enables the vertically integrated firm to leverage its market power and there are no pro-competitive rational justifying the behaviour. [157]Although recognizing that self-preferencing cannot be abusive *per se*, the report argues that the practice should be subject to an effects test. Accordingly, if the vertically integrated dominant platform is an intermediary infrastructure and regulates its ecosystem, the platform will have to prove that its self-preferencing practices have no long-run exclusionary effects in downstream markets. [158]

[156] *Supra* note 96, at 182-184.
[157] Supra note 3, at 7.
[158] *Id.*

4. Platforms as de facto privacy regulators: Google Sandbox and Apple ATT case

4.1) Apple ATT case

Apple Inc., headquartered in Cupertino, California, and listed on the New York Stock Exchange, leads a group of companies engaged in the design, production, and marketing of mobile communication and multimedia devices, personal computers, and audio-video devices under the Apple and Beats brands. Additionally, Apple is involved in the sale of a wide range of software, services, peripherals, and related networking solutions, as well as third-party applications and digital content.

Starting in April 2021, Apple, as the owner of the iOS operating system, imposed a privacy policy on competing app developers using its online store, the "App Store." This App Tracking Transparency (ATT) policy mandated stricter rules for user privacy protection compared to those Apple applied to itself.
The differential treatment was primarily based on: i) the characteristics of the "pop-up window", or a prompt, appearing to users for the purpose of obtaining consent for tracking their internet browsing data; ii) the tools used for measuring the effectiveness of advertising campaigns.
Specifically, the formulation of the prompt that Apple imposed on third-party app developers: a) presented the options to "deny" or "grant" consent in a way that visually favored the former; b) used the phrase "permission to track (emphasis added) your activities across other companies' apps and websites" without providing any explanation of the term "track," which could easily be a source of concern and deterrence for the user; c) did not emphasize the benefits of personalized advertising for users.[159]

Conversely, when it came to apps developed directly by Apple, the corresponding prompts prominently displayed the positive option of granting consent. Moreover, the

[159] AGCM Decision No. 30620 of May 2, 2023, Case A561 - Apple App Tracking Transparency Policy;

consent sought in Apple's prompts pertained to "personalized services" rather than "tracking" user activities.

Even in scenarios where users granted consent for "tracking," third-party app developers were still restricted from sharing the same data to enable ad personalization and effectiveness measurement across different apps. Apple's ATT system required a so-called "double explicit consent," stipulating that consumers had to provide consent for tracking each time they accessed different apps, even if the apps were interconnected. This "double explicit consent" was not required for apps developed by Apple. [160]

As a consequence of the aforementioned measures, the consent rates of users shown the ATT prompt in competiting apps, available through the App Store, dropped significantly. This discrepancy in consent acquisition also affected the measurement of advertising campaign effectiveness, placing third-party operators at a disadvantage compared to Apple. Specifically, SkadNetwork, the application programming interface (API) provided by Apple to third-party advertisers and app developers for measuring ad campaign effectiveness, had technical charachteristics making it less useful and significantly less effective compared to Apple Ads Attribution, the advertising tool used by Apple. The limitations of SkadNetwork, even in its updated versions, included:

1. Delayed access to conversion data (with a minimum delay of 24-48 hours), while Apple Ads Attribution provided immediate data access.
2. The data provided by SkadNetwork was limited and overly aggregated, making it inadequate for revealing users' actual preferences. In contrast, Apple Ads Attribution provided advertisers with detailed data such as the user's country or region, the date and time of the click, and the ad associated with the app installation.[161]

Before Apple's adoption of the ATT policy, competitors could offer a variety of tools independently, to help advertisers measure ad campaign effectiveness. These tools allowed access to metrics for ad reporting, audience, and conversions, providing granular and real-time information about the performance of advertising campaigns.

[160] *Id.*, paragraph II, sections 12-14;
[161] *Id.*, paragraph II, sections 15-16;

However, following the implementation of the ATT policy, the reduced ability to profile users led to an increase in the "cost per action" (CPA) for advertisers purchasing ad space on competing apps. The higher costs for advertisers resulted in a decreased willingness to purchase ad space, leading to a significant reduction (over 50%) in the revenues of third-party app developers.[162]

Based on these premises, the Italian "*Autorità garante della concorrenza e del mercato*" (AGCM), opened an investigation into Apple's conduct, focusing on the discriminatory nature of its privacy policies and their potential anticompetitive effects, as a violation of Article 102 of the Treaty on the Functioning of the European Union (TFEU). To evaluate a potential abuse of a dominant position, the Authority proceeded to identify the product and geographic scope of competition between enterprises (relevant markets), the market power held by the enterprises (dominant position), and the conduct that may constitute the anticompetitive practice.[163]

The relevant product markets, in this case, were identified as those allowing Apple to influence user data collection on the iOS platform and monetize such data for personalized advertising and app funding. The common element of these activities thus resided in Big Data. These markets included:
a.1) The market for platforms for the online distribution of apps for users of the iOS operating system, where the assessment of dominance was conducted;
a.2) The market for the development and distribution of apps;
a.3) The markets for online advertising;
a.4) The market for the production and sale of high-end mobile devices.[164]

The App Store is characterized as a two-sided platform that intermediates and facilitates transactions between two distinct groups of users: (i) developers who distribute their apps to end consumers using the iOS operating system on their mobile devices, and (ii) consumers who seek apps to download, either for free or for a price, onto their mobile devices. The two sided of the platform were considered as distinct product markets. The

[162] *Id.*, paragraph II, sections 17-18;
[163] *Id.*, paragraph III, section A;
[164] *Id.*, paragraph III, section B;

rules governing privacy consent requests (ATT policy) within the iOS system were enforced by Apple onto developers. Therefore, the relevant market for evaluating Apple's conduct was where it provided access to its App Store. [165]

This analysis involved assessing the substitutability from both the demand and supply sides, as well as Apple's dominant position. The App Store stood as the exclusive online store for the distribution of native apps to iOS users, as Apple prohibited the download of apps for iOS devices through alternative stores. Concurrently, web apps were not accessible through the iOS mobile operating system. The alternative option, Google Play Store, was not a viable substitute from developers' perspective, as it catered solely to Android users. In fact, as smartphone users tend to use only one device, app developers are compelled to offer their applications on both iOS and Android systems. In conclusion, there appeared to be no available alternatives to Apple's App Store that could serve as substitutes for app developers intending to offer their apps to iOS users. Regarding supply-side substitutability, no other providers could offer a distribution platform to rival the App Store due to Apple's tight control over its ecosystem.[166]

From a geographic standpoint, the market for distribution platforms for iOS applications was considered global, with Apple being the sole provider across all countries. Furthermore, Apple enforced consistent rules across all EU Member States, explicitly prohibiting developers from distributing apps through alternative online stores for iOS devices. [167]

Given these considerations, it resulted unequivocal that Apple held a dominant position, at national and international level. [168] Persuant to the AGCM, by exploiting its dominant (monopoly) position in the market for online app distribution platforms for iOS users, Apple adopted a discriminatory policy of self-preferencing that likely resulted in:

i) Reducing third-party advertisers' revenue while favoring Apple's commercial division, particularly by favoring its direct sales and its advertising intermediation platforms;

[165] *Id.*, paragraph III, section B.1, 24-25;
[166] *Id.*, paragraph III, section B.1, 26-28;
[167] *Id.*, paragraph III, section B.1, 29;
[168] *Id.*, paragraph III, section C, 43;

ii) Reducing the entry or preventing the continued presence of competitors in the app development and distribution market, due to the alteration in the remuneration prospects of competing apps;
iii) Advantaging Apple applications and, consequently, Apple mobile devices and the iOS operating system.[169]

Indeed, the availability of user data and profiling, while respecting privacy protection regulations, are essential elements for the attractiveness of advertising spaces purchased by advertisers because they:
i) Allow advertising to be directed to specific consumers (based on their online behavior, interests, and demographic data), who are more likely to purchase the advertised products or services or install new apps;
ii) Enable the measurement of the effectiveness of advertising campaigns over time, for example, by identifying the percentage of conversions into sales.[170]

By introducing the ATT policy exclusively for third-party app developers, Apple discriminatorily reduced the ability of publishers, app developers, and competing ad networks (on the supply side) to profile users, thereby reducing the value of advertising for advertisers served by them (on the demand side) and consequently hindering— to its own advantage—the competitors' ability to sell advertising space.
In this context, the issue was not the *level* of privacy chosen by Apple within its digital ecosystem, but rather the choice to adopt differentiated (and potentially discriminatory) privacy policies between itself and its competitors. The disadvantageous position of third-party apps resulting from the ATT policy would therefore push consumers to increasingly rely on both Apple devices and apps, thereby hindering the transition of users towards purchasing devices equipped with the competing operating system. [171]

In conclusion, the AGCM is currently assessing whether Apple's enforcement of the ATT policy on third-party developers, while exempting its own applications, could constitute an abuse of its dominant market position and a violation of EU competition

[169] *Id.*, paragraph III, section D, 44;
[170] *Id.*, paragraph III, section D, 45;
[171] *Id.*, paragraph III, section D, 46-47;

laws. This conduct by Apple, allegedly aimed at self-preferencing and disadvantaging competitors, is suspected of harming the competitive landscape. Such an outcome could reduce consumer choice and increase costs in the app development and distribution sectors. It is important to note, however, that the AGCM has not yet reached a definitive conclusion on this matter.

Nevertheless, this case, along with the Privacy Sandbox case analysed in the subsequent section, offers the possibility to reflect on the use of data privacy as a justification for anticompetitive conduct, which creates a new facet of interaction between antitrust and data privacy law. At the same time, the case enables a first understanding of the different perspectives adopted by competition and data protection authorities: the former looking at the anticompetitive implications of the adoption of differentiated privacy policies, and the latter focusing instead on the level of privacy granted to consumers.

4.2) Google Sandbox case

As previously emphasised throughout this work, recent years have seen regulatory efforts to improve user privacy, culminating in legislative instruments such as the GDPR or the CCPA, as well as increased privacy awareness among users. At the same time, popular browser vendors have taken concrete measures to clamp down on cross-site tracking, putting pressure on Google to follow their example. On its part, Google had signaled on various occasions that it would gradually take steps to limit user tracking in Chrome.

First, in May 2019 Chrome announced a series of measures that would make it easier for users to delete third-party cookies without losing their log-in information, while making it harder for trackers to fingerprint users. Then, on 22 August 2019 Chrome announced an open source initiative – the Privacy Sandbox – whose goal is to develop a new set of web standards "to fundamentally enhance privacy on the web," while at the same time supporting a vibrant ad-funded web ecosystem. [172]

[172] *Supra* note 11 at 37-38;

The Privacy Sandbox proposals are a series of browser Application Programming Interfaces (APIs) which would satisfy advertising use cases without relying on third-party cookies, furthermore mitigating opaque workarounds such as fingerprinting. Eventually, in January 2020 Google announced plans to phase out third-parties cookies access on is Chrome web browser within two years. Google developers also signalled Chrome's intention to engage with the wider online community, inviting all interested stakeholders (e.g., browser makers, ad tech vendors, publishers, advertisers) to submit observations and feedback on GitHub and through the World Wide Web Consortium ("W3C"), a body responsible for setting web standards.[173]

The Privacy Sandbox's proclaimed goal is to enhance user privacy on the web, while at the same time preserving the ad-funded business model. However, this change lays down a very different vision of web advertising: as part of the new policy, Chrome would use algorithms to create many "cohorts", namely groups of people sharing certain features. A person's browsing history would be kept private, but the browser would look at the history and assign each user to a particular cohort. When a user visits a website, Chrome will tell that website the cohort that individual belongs to. Advertisers and publishers currently have access to such cookies, and rely on them to deliver online advertising. This business policy makes it more difficult for advertisers to track users' activities on the web, as instead of having individualized and detailed information, they would only have aggregate information. This implies that platforms would not have the same ability to serve well-targeted ads, and advertisers' willingness to pay would decrease.[174]

The various Privacy Sandbox proposals may thus be considered a form of client-side privacy- enhancing technologies, preventing publishers from enriching user profiles with user activity on third party websites. Even so, an important caveat should be made at this stage. Chrome's vision leaves intact the ability of publishers to individually identify users when these are visiting their online properties – either through a user log-in or a first-party cookie. Hence, when this publisher happens to operate multiple leading consumer facing services – as Google, that operates more than 50 such

[173] *Id.,* at 39-40;
[174] *Supra* note 2, at page 9, section 3.1.3;

services– the ability to observe and combine user activity across different services to create a user profile will not be removed. [175]

Under this approach, there are no boundaries between Google's platform and the "open web"; insofar as the user browses through Chrome, the open web becomes part of Google's logged-in environment. The Privacy Sandbox thus kills third-party cookies, but it does nothing to curtail the tracking taking place on platforms where surveillance is arguably most pervasive: Google and Facebook.

Most experts consider that first party data can be a credible solution only for very large publishers that boast vast user bases.[176] The same concern was raised by the CMA: "large incumbent platforms with leading consumer-facing services like Google and Facebook are significantly less dependent on third-party cookies for delivery of high-performing targeted ads and continued advertising revenues than, for instance, small publishers with free-to-read content that does not require log-in."[177]

As previously highlighted, the "walled gardens" of Google and Facebook are beyond any comparison with other publishers in terms of breadth and depth of their data; these companies happen to operate some of the world's most popular consumer-facing services, which allow for the extraction of rich data signals such as purchase intent or emotional state, and are able to combine such data across services to create super-profiles. On balance, it seems that leveraging first-party data will likely favour a handful of high-scale publishers, and is unlikely to serve as a valid replacement for third-party cookies for small- and medium-size publishers.[178]

Both privacy and competition agencies are watching closely as Google makes this change. On the privacy side, there is some cautious optimism that the blocking of cookies may signal broader change toward more privacy-protective models within the online advertising ecosystem. The likely privacy effects, whether positive or otherwise,

[175] *Supra* note 11, at 41-42.
[176] *Id.*
[177] CMA, Online Platforms and Digital Advertising market study, Appendix G: the role of tracking in digital advertising (2020) [online] Accessible at: https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf
[178] *Supra* note 11, at 56-57.

will ultimately depend on the alternative technology that Google introduces to replace third-party cookies. Antitrust authorities view Google's changes as more uniformly negative for competition: there is in fact the risk that the Privacy Sandbox rules would not apply to Google itself, which may continue to have detailed information about users, and may therefore entrench Google's dominance in digital advertising. Though best understood as a competitive foreclosure allegation, the claims can be described as Google "self-preferencing," as the platform's own advertising tools will have access to tracking data that third parties will no longer be able to collect directly.[179]

The UK's Competition and Markets Authority saw potential anti-competitive concerns and, in conjunction with the UK privacy authority, investigated the conduct at issue:
"[...] the CMA is concerned that [...] the Privacy Sandbox Proposals would allow Google to:
(a) distort competition in the market for the supply of ad inventory in the UK and the market for the supply of ad tech services in the UK, by restricting the functionality associated with user tracking for third parties, while retaining this functionality for Google;
(b) *self-preference* its ad inventory and ad tech services by transferring key functionalities to Chrome, providing Google with the ability to affect digital advertising market outcomes through Chrome in a way that third parties cannot scrutinise, and leading to *conflicts of interest*; and
(c) exploit its *apparent dominant position* by denying Chrome web users substantial choice in terms of whether and how their personal data is used to target and deliver advertising to them.
These concerns relate to the impact of Chrome's policy change on competition among publishers for advertising revenue (i), and on ad tech vendors(ii). [180]

(i) Impact of competition among publishers
On one hand, Google is in a vertical relationship with publishers, in that it is the leading provider of ad tech tools publishers use to monetize their inventory. It also operates

[179] *Supra* note 107, at 104 and 115.
[180] Competition and Markets Authority, 2022a. Case number 50972, 11 February 2022, page 23.

Chrome, which in the near future could perform functions currently undertaken by ad tech vendors. At the same time, Google happens to offer some of the most coveted online ad spaces, such as YouTube, Maps, Gmail, and of course Google Search. In this sense, Google is also a publisher competing horizontally for ad dollars with its customers. [181]

When Google operates as an ad tech intermediary, it receives a fraction of ad spend – which Google itself claims to be around 31%. On the other hand, when it operates as a publisher, Google receives 100 cents to the dollar, since it sells its owned and operated inventory exclusively through its own ad tech tools. This means that Google is better off in financial terms – at least in the short run – if advertising demand shifts to its owned and operated properties at the expense of the open web. The concern is that Google would leverage its market power as the dominant browser to give itself an advantage as a publisher, thus distorting competition in the market for online display advertising. [182]

As the CMA observed, "to the extent that targeted advertising on open display inventory is less feasible or effective without third-party cookies, advertisers may substitute spending away from open display advertising and towards advertising on platforms' owned-and-operated inventory."[183] If marketers shift their spending to the walled gardens of Google and Facebook, these companies will capture an even greater share of the online advertising pie at the expense of open web publishers. Few would disagree with the proposition that Google does not have an incentive to annihilate the open web, but the fact that Google relies on publishers in the aggregate does not mean its incentives are aligned with theirs and no antitrust concern may arise. [184]

Some commentators, in trying to find a rational behind Google's allegedly exclusionary practices, have turned to the consideration of the model of imperfect rent extraction: it is the business model based on monetisation through advertising that reduces the platform's ability to extract rents from third parties which make use of its inputs. In turn, the platform may have the incentive to foreclose them and increase sales with its own services.[185] Thus, the CMA's concerns about a possible anti-competitive impact of Google's proposed policy might have a very similar rationale as in the Google

[181] *Supra* note 11, at 62.
[182] *Id*.
[183] CMA, Online Platforms and Digital Advertising Market Study, paragraph 5.325.
[184] *Supra* note 11, at 63.
[185] *Supra* note 2, page 9, section 3.1.3.

Shopping case.[186] In the present case, Google would be using its dominant position in one market (e.g., the market for browsers) to extend it to an adjacent market (e.g., the market for online display advertising) by having recourse to methods that do not constitute competition on the merits and which are capable of restricting competition.[187]

(ii) Impact of competition among tech vendors

The second set of leveraging concerns relates to the effects of Chrome's policy change on competition among ad tech vendors. For years, Google has been the leading (and possibly dominant) provider of ad tech tools across the value chain, namely publisher ad servers, ad exchanges/SSPs, demand side platforms and advertiser ad servers. [188]

As the CMA explained, throughout the years Google has engaged in a variety of leveraging practices in the ad tech ecosystem; furthermore, the platform has the ability and incentive to leverage market power from one level of the ad tech value chain to another. Google was held to satisfy all the conditions for conflicts of interests to be problematic, one of them being that Google is overwhelmingly the largest provider in publisher ad serving, while also operating the largest demand side platform. [189] As explained above, the various Privacy Sandbox proposals cede ultimate control to the browser, which, rather conveniently for Google, will be Chrome in most cases.

The CMA examined two potential scenarios for the future of ad intermediation, one whereby the way the auctions are run does not substantially change (i.e. the ad server remains the final decision maker) and one where the browser executes at least some of the auctions. It held that in both cases its analysis on conflicts of interests would remain valid. [190]A decrease in competition among ad tech providers can result in considerable welfare losses, as it can translate in less innovation, lower quality and higher prices for customers, namely publishers and marketers. In turn, such effects can be felt on by end users, either in the form of less free (or lower-quality) ad-funded content online, or in the form of higher prices for the marketer's goods or services.[191]

---

[186] *See* supra note 2, at 6-7, section 3.1.1.
[187] *Supra* note 11, at 64.
[188] *Id*., at 67.
[189] CMA Online Platforms and Digital Advertising Market Study (July 1, 2020), paragraphs 5.261-5.272.
[190] CMA, Online Platforms and Digital Advertising Market Study, Appendix M: intermediation in open display advertising, paragraphs 540 and 543.
[191] *Supra* note 11, at 69.

In short, the proposed change eliminates direct access to competitively-important cookie data, which advertisers and publishers currently use to compete with Google in ad delivery and ad tracking. The concern is that this shift would tighten Google's control over ad data, insert Google into the ad supply chain as a new and necessary intermediary for its competitors, and ultimately raise barriers to competition. [192]

In February 2022, the CMA accepted Google's revised commitments, according to which Google would restrict data sharing within its ecosystem not to benefit itself when third-party cookies are removed.[193]

The latest quarterly report from the CMA (04/26/2024) sets out the progress made to date, including the CMA's latest views on the potential impact of Google's proposed Privacy Sandbox changes condensed in more than 79 concerns.[194] The CMA's report states: "Although there are a number of concerns to work through, based on the available evidence, we consider that from 1 January 2024 to 31 March 2024 (the relevant reporting period), Google has complied with the Commitments. This means that in our view Google has followed the required process set out in the Commitments and is engaging with us (and the ICO) to resolve our remaining concerns ahead of third-party cookie deprecation. However, further progress is needed by Google to resolve our competition concerns ahead of deprecation." [195] The report also takes into account the Information Commissioner's Office's provisional views and reflects its outstanding concerns to ensure that both competition and privacy are protected.

This Google example reflects a more general policy concern, that dominant firms may self-preference their vertically integrated services in the interpretation of privacy obligations. In particular, Chrome and Apple' s policy changes raise issues of accountability, as the platorms get to decide on the right trade-off between privacy and efficiency for a whole industry. This relates to one of the main themes of this work, namely that these platforms purport to act as *de facto* privacy regulators-relying on privacy as a justification for anticompetitive conduct.

---

[192] *Supra* note 107, at 105.

[193] Competition and Markets Authority, 2022a. Decision to accept commitments offered by Google in relation to its privacy sandbox proposals. Case number 50972, 11 February 2022.

[194] Competition and Markets Authority, Q1 2024 update report on implementation of the Privacy Sandbox commitment.

[195] Competition and Markets Authority, Q1 2024 update report on implementation of the Privacy Sandbox commitment, Summary, section 4.

5. Privacy and Competition Trade-off

5.1) Data privacy as a justification for anticompetitive conduct

Though rare and early-stage, antitrust cases and policy discussions have begun to raise the question of whether the protection of individuals' data privacy could justify otherwise anticompetitive conduct by a firm. This newly emerged theme reflects a new facet of interaction between antitrust and data privacy law. [196]

The two policy changes at the center of this discussion were premised on the rational of allegedly enhancing data protection and user privacy. The Commission has traditionally expressed skepticism when companies have invoked the health and safety of consumers to justify their conduct, holding that such interests are safeguarded by regulators, not private undertakings. [197]

Under EU privacy laws, end users already have to freely consent to the use of their data for advertising purposes based upon all relevant information.

If Apple used the tools already available today as it pledges and openly advertises – to block access to the App Store for those apps that do not comply with EU privacy laws – there would not be an issue. Apple has failed to present convincing evidence that the tracking prompt is necessary to preserve end users' personal data. Neither has it explained how presenting end users with a two-sentence "yes or no" prompt to block an app developer's third-party tracking is meant to increase end users' data sovereignty where many more options and variations exist. However, even if one were prepared to assume a privacy interest in Apple's tracking prompt that Apple can claim on behalf of end users, this does not automatically mean that such interests outweigh the interests in continued competition, and thereby immunizes the conduct from antitrust scrutiny. [198]

[196] *Supra* note 107, at 126-127.
[197] *See* Case T-30/89, Hilti AF v Commission [1991] ECR II-1439, paragraph 118.
[198] Höppner, Thomas and Philipp Westerhoff. "Privacy by Default, Abuse by Design: EU Competition Concerns About Apple's New App Tracking Policy". *Hausfeld Competition Bulletin* (2021), Available at SSRN: https://ssrn.com/abstract=3853981 or http://dx.doi.org/10.2139/ssrn.3853981

Similar arguments can be expressed for the second case at hand: even if one accepts that privacy can be a legitime objective on which Google may rely to justify its conduct, it would still be possible to show that there are less restrictive alternatives which Google could have pursued to promote user privacy. Google could argue that irrespective of its public good character and its wider societal implications, privacy is at the same time an important quality parameter of its products. An increase in user privacy could thus be seen as an improvement in quality which allows Google to differentiate itself from competitors and represents a welfare gain for consumers. [199]The argument would then be that any exclusionary effects from Chrome's policy change are overridden by the increased quality benefits for consumers. This is ultimately an empirical issue, to which no easy answer can be given; one would need to examine whether the increase in quality would outweigh the welfare losses from Chrome's policy change, including losses for publishers (less ad revenue), marketers (increased media waste) and ultimately consumers. Nevertheless the prior analysis of the case points out that the privacy benefits of Chrome's policy change may actually be much smaller than what one would initially think, for the reason that such change would do nothing to curb online tracking on platforms such as those offered by Google and Facebook. [200]

Antitrust and data privacy agencies have also recognized a related policy concern—that dominant digital platforms may have the power and ability to over-interpret the privacy obligations they impose on other market participants, as a means to exclude competitors and entrench their own market power. [201]

In a report concerning large digital platforms, The U.K. competition authority has referred to Google's plan to terminate third-party cookies as "a further example of platforms' increasing role in deciding on the appropriate application of data protection regulation for other market participants." [202] Furthermore, the authority stated that they ". . . have an incentive to interpret data protection regulations in a way that entrenches their own competitive advantage, including by denying third parties access to data that is necessary for targeting, attribution, verification and fee or price assessment while

[199] *Supra* note 11, at 65-66.
[200] *Id*.
[201] *Supra* note 107, at 132.
[202] Competition & Markets Auth., Online Platforms and Digital Advertising Market Study, at 5.328 (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

preserving their right to use this data within their walled gardens". [203] In the same report, the authority expressed more pointedly that the concern is that platforms "have a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within their own ecosystems. . . . [T]his may even create an artificial incentive in the long run towards greater vertical integration." [204]

Claims of data privacy as a business justification present an opportunity for productive collaboration between antitrust and data privacy authorities. The expertise of data privacy authorities could provide insight to antitrust authorities in their factual determination of whether privacy protection or interests are truly at stake, and to ensure an accurate understanding of the scope of protected privacy interests.

5.2) Shared policy interests, conflicts and possible synergies

Despite often being summarized as complementary or in tension, the relationship between antitrust law and data privacy is more nuanced. Each legal realm has its own distinct objectives through which it pursues such consumer benefits: privacy law seeks to protect individual's data privacy rights and interests, while antitrust law works to ensure efficient competition in the marketplace.[205]

Around the world, one of the most widely articulated objectives of antitrust law is to improve consumer welfare through competition. This consumer welfare goal is typically expressed in legislation in terms of economic efficiency, though the concepts of welfare and efficiency are not necessarily synonymous. Competition law seeks to benefit consumers through a broad, economic efficiency prescription, rather than the individualized rights or interests that are characteristic of privacy law. [206]
The different objectives of each regime are also reflected in the breadth of the policy framing—antitrust agencies tend to investigate policy issues on somewhat broader

[203] CMA Online Platforms and Digital Advertising Market Study, *supra* note 202, at 293.
[204] *Id.* at 296.
[205] *Supra* note 107, at 36.
[206] *Id.* at 36-38.

terms, such as several recent "digital policy" or "digital platforms" reports. This broader framing often makes sense in light of antitrust authorities' more general, economic efficiency goals. [207]

Apple and Google's policy changes highlight the different policy perspectives of antitrust and data privacy, raising complex issues. Though somewhat simplified, the agency responses to Google so far illustrate that competition policy tends to encourage the flow of data in digital environments, as a means to promote data-driven competition, while data privacy policy often leans toward added controls or limits on such data flow.[208] This policy tension presents an opportunity for productive discussion and collaboration between antitrust and data privacy authorities.[209] First, it may be helpful to identify and understand whether (and when) there are truly policy choices or tradeoffs between the promotion of competition and the protection of data privacy. It may be that on closer examination, the interests are not in opposition, and both can be pursued.[210]

Indeed, despite having distinct enabling legislation and mandates, competition and data privacy authorities share a number of common policy interests. [211] There is a shared policy interest in fostering conditions that promote trust in markets, as a means of encouraging market participation. Privacy agencies emphasize the building of trust between individuals and businesses (as well as government) within their mandates and strategic priorities. They furthermore describe the importance of building individual's trust that firms will process their data in accordance with data protection laws as a means to encourage consumer participation in markets, and a vibrant economy. Competition authorities similarly emphasize the importance of trust and confidence in markets. Consumer trust in businesses is seen as a precursor to the robust economic participation and competition that drives consumer welfare. Conversely, where there are trust-eroding market conditions—such as information asymmetries, a lack of

[207] *Id.*, at 36-41.
[208] *Id.*, at 105-106.
[209] CMA Online Platforms and Digital Advertising Market Study, *supra* note 202, at 5.330 (noting the same).
[210] *Supra* note 107, at 105-106.
[211] *Id.*, at 44-47.

transparency in pricing practices or anticompetitive conduct—this reduces consumer trust, confidence and engagement in the market.[212]

Data portability rights have become one of the most-emphasized areas of complementarity between data privacy law and competition policy. As part of their data privacy legislative objectives, several jurisdictions emphasize the free movement of data. For example, the GDPR prevents restriction of "the free movement of personal data" within the European Union. At the same time, data movement can play a central role in enabling competition, particularly in the digital economy: data portability rights make it easier and more likely that consumers will switch between data-driven service and enables new competitive entry and expansion by making it easier for entrants to win over customers (and their data) from incumbent firms. [213]

A third aspect of complementarity resides in the common policy objective to promote consumer choice in markets, although for different reasons. Consumer choice, often in the form of notice and consent, has long been a central principle within privacy law. At the same time, antitrust law seeks to combat anticompetitive conduct and mergers, both of which can reduce consumer choice in markets.[214] In some instances, if the concentration of personal data among few providers eventually reduces consumer choice and control over privacy, privacy and competition interests may coincide over the long term.[215]

To the extent tradeoffs are thought to exist between the two interests, it would be helpful for antitrust and data privacy authorities to jointly discuss how each realm views the appropriate and productive balance between the promotion of privacy and competition. The U.K.'s cross- agency consideration of the Google cookies change is an example of this type of collaboration.[216]

Though there are likely to be justified and logical differences in the views of each agency, the discussion remains useful to promote deliberate and careful cross-doctrinal

[212] Id., at 44-47.
[213] *Id.,* at 48-55.
[214] *Id.,* at 55-56.
[215] CMA Online Platforms and Digital Advertising Market Study, *supra* note 202, at 5.328.
[216] *Supra* note 107*,* at 106.

understanding— without this collaboration, there may be unwitting or unintentional tradeoffs, where one realm pursues its interests at the cost of the other. In the absence of shared agency thinking on this subject, digital platforms will be left with the power and ability to decide the balance between data access that promotes competition, and data control that protects privacy.[217]

Despite the interaction of antitrust and privacy law being complex, new, and often under-theorized, various subject areas exist where collaboration between antitrust and data privacy authorities would be particularly valuable. These high-priority topics for future cross-agency discussion include:

- Privacy and competition trade-off

There may be tradeoffs between promoting competition and protecting data privacy in law, enforcement, or policy. Understanding when and to what extent these tradeoffs occur is crucial. Where tradeoffs exist between data-driven competition and data protection, cross-agency discussions are necessary to determine the appropriate balance between these interests.[218]

- Privacy Quality and Competition

The quality of privacy protection within a market is likely to be influenced by competition. Understanding how this privacy quality is affected, and how data privacy protection might, in turn, affect competition, is essential. Antitrust and data privacy authorities should discuss and develop understandings of when privacy-based competition impacts the privacy features and quality of products in specific markets.[219]

- Measuring Competitive Effects on Privacy

In practical terms, antitrust authorities need to measure the relevant effects of competition on the quality of privacy offered in a given market. Recent developments in antitrust quantification of quality-based effects are minimal. Methods and tools for measuring the effects of competition on privacy are still in early stages but are crucial for integrating privacy considerations into many aspects of antitrust analysis.

[217] *Id.*
[218] *Supra* note 107, at 144.
[219] *Id.* at 145.

Collaboration between data privacy and antitrust authorities is significant for developing reliable methodologies and tools to measure competition-related effects on privacy quality. Privacy authorities' expertise in evaluating privacy and market conduct effects could provide important insights for antitrust evaluations.[220]

- Abuse of Dominance

The relationship between monopolization, competition, and privacy needs to be understood. Monopoly power, or competition, can affect the privacy protections offered to consumers. Some cases allege that monopoly power reduces the quality of privacy services in certain markets. This presents an opportunity to develop a deeper understanding of the relationship between monopolization and privacy through evidence-based approaches.[221]

- Business Justifications

The protection of data privacy is sometimes used to justify otherwise anticompetitive conduct. Antitrust authorities need to evaluate claims that a merger or misconduct was conducted to protect data privacy. Collaboration between antitrust and data privacy authorities is beneficial in assessing such claims. Privacy expertise can inform antitrust determinations of legitimate privacy interests and ensure an accurate understanding of the scope of these interests in specific cases. It is also useful in determining whether companies are over-interpreting data privacy compliance obligations to limit competition. [222]

- Assessment and Development of Theories and Practice

Existing theories on antitrust and data privacy need to be tested and developed in enforcement and litigation to ensure they are well-founded, evidence-based, and sufficiently broad to explain the various interactions between the two areas of law. Recognizing this nascent intersection of law, it is important to consider how

[220] *Id.,* at 145.
[221] *Id.,* at 146.
[222] *Id.*

developments in data privacy or antitrust law (or policy) might affect the interactions between these realms.[223]

This intersection of law is rapidly developing, and continuous evaluation is necessary as theories are tested, developed, and expanded in cases and enforcement. Around the world, some jurisdictions are passing their first data privacy laws, and existing laws are being expanded through new amendments and enforcement actions. Simultaneously, antitrust law is being amended with a focus on greater digital enforcement, and antitrust agencies are bringing novel cases against digital platforms. This expansion of both areas of law may create new or more extensive interactions between them, as well as with consumer protection law. As several jurisdictions consider and introduce *ex-ante* digital sector regulation, both antitrust and data privacy agencies may find themselves collaborating with new agencies or laws affecting this shared space.[224]

5.3) *Ex-ante* regulation: the Digital Markets Act

Whereas the discussion about integrating privacy in traditional competition law is a still emerging debate within a group of competition scholars, the current discussion about new and partly fundamental reforms in competition policy for addressing the huge challenges of the large tech firms is in the center of the academic and public debates and the legislators in the European Union, the United States, and many other countries. This debate has led in the European Union to the currently discussed "Digital Markets Act" (with its new ex-ante regulatory approach), the various proposals for new antitrust bills in U.S. Congress, and other far- reaching legislative proposals in other countries.[225]

All of these reports clearly emphasize the importance of the collection and use of huge amounts of personal data of consumers for the business models of large digital firms with their platforms and ecosystems. This refers not only to their use for targeted advertising, but also to the manifold other ways how comprehensive consumer profiles can be used in many different markets. All the reports agree that the main problem is the

[223] *Id.* at 147.
[224] *Id.*, at 144-148.
[225] *Supra* note 13, at 288-289.

concentration tendencies through the economic characteristics of digital platforms with their large economies of scale and direct and indirect network effects. However, also the control over huge amounts of personal data through the large tech firms is seen as a key factor for the economic power of these firms, especially through raising barriers to entry and the manifold strategic options for using these data to leverage their market power into other markets. Therefore, the main focus in these reports was on the impact of this data collection on entrenching the market power of the large digital platforms, and, thus, on the effects on competition. [226]

The effects of this economic power of large tech firms on the privacy (and informational self-determination) of consumers, for example, also with respect to excessive collection of personal data by the large digital platforms, was not part of these investigations and analyses. Also the lack of control of consumers over their data, especially through information and behavioral problems, has not been in the center of these reports, although they are often mentioned as an important additional problem. Therefore, neither the privacy problem nor the information and behavioral market failure problem have been targeted by these reports and the proposed policy solutions. [227]

It is, however, interesting that in some of these reports, and in the ensuing more general discussion "fairness" considerations, and therefore distributional aspects have got more and more attention also for dealing with the power of the large digital platforms.With regard to the economic power of the large tech firms, the policy proposal of the Furman report turned out to have been the most influential. It claimed that traditional EU competition law with its ex-post control of abusive behavior of dominant firms (Art. 102 TFEU) is too slow and not effective enough. It therefore recommended to introduce an ex-ante regulatory approach with an additional set of rules for this small group of firms (which were seen as having "strategic market status").[228] After long deliberations, this idea of an additional ex-ante regulatory approach was also used by the European

[226] *Id.*
[227] *Id.*
[228] For the Furman proposal about an additional "digital market unit" that can decide also on "codes of conduct" for digital platforms with a "strategic market status," see Digital Competition Expert Panel, *Unlocking Digital Competition*, Furman Report (Mar., 2019), , at 54–63; https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel;

Commission for its DMA proposal (published in December 2020).[229] According to this DMA proposal, the EU legislator would subject gatekeepers that provide core platform services to overall eighteen (self-executing) obligations regarding their conduct, i.e. directly applicable (Article 5), and a list of obligations that may be further specified by the Commission (Article 6). Following the initial proposal of the European Commission in December 2020, the Regulation was adopted by the European Parliament and the Council on 14 September 2022, and was implemented on 7 March 2024. It provides a set of clearly defined, objective criteria for an undertaking to classify as a gatekeeper, defined in Article 3 of the Regulation. [230]

The DMA has two overarching aims: contestability, defined in Recital 32 as "the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services" and fairness, as far as the regulation is concerned with both "business users and end users of core platform services provided by gatekeepers in particular." (Recital 7).[231] The DMA focuses on digital services that feature "extreme scale economies, very strong network effects, an ability to connect many business users with many end users through the multi-sidedness of these services, lock-in effects, a lack of multi-homing or vertical integration" (Recital 13). The concern about gatekeeper platforms stems from the claim that undertakings providing certain core platform services have "gained the ability to easily set commercial conditions and terms in a unilateral and detrimental manner for their business users and end users" (Recital 13). While several commercial conditions have differential impacts on business users and end users), self-preferencing is a candidate for harming third-party sellers and end users alike. [232]

[229] European Commission, Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act);
[230] On 6 September 2023 the European Commission designated for the first time six gatekeepers - Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft.
[231] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66; *hereinafter* "Digital Markets Act".
[232] Peitz, Martin. "How to Apply the Self-Preferencing Prohibition in the DMA." *Journal of European competition law & practice* 14, no. 5 (2023): 310–315.

As highlighted by recital 32, the prohibition of self-preferencing can be derived from the overarching aim of contestability: "The features of core platform services in the digital sector, such as network effects, strong economies of scale, and benefits from data have limited the contestability of those services and the related ecosystems. Such a weak contestability reduces the incentives to innovate and improve products and services for the gatekeeper, its business users, its challengers and customers and thus negatively affects the innovation potential of the wider online platform economy." [233] Favouring first-party products and services can be seen as distorting the competition between the various undertakings in a sector and may limit the contestability of the market. For example, if a gatekeeper reduces the visibility of superior third-party offers, third-party sellers have weaker incentives to provide such quality in the first place. Similarly, if any effort in cost reduction by a thirdparty seller is offset by an equivalent increase in fees charged by the gatekeeper, third-party sellers do not have an incentive to reduce their costs. A differential treatment of first-party and third-party offers may be deemed unfair. While there are different notions of fairness, and self-preferencing should primarily be seen as a contestability issue, it may also be argued that fairness is violated if business users could not fully anticipate a differential treatment when making their participation or investment decisions. [234]

Among the obligations subject to further specification by the Commission, some are noteworthy for the purpose of this analysis. The prohibition of the exclusionary conduct that is the focus of this dissertation, namely self-preferencing, comes from Article 6(5) of the DMA, albeit in a narrow sense, as it prohibits only practices related to ranking, indexing and crawling services: "gatekeepers should not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking and related indexing and crawling."[235] Some commentators have pointed out how despite the explicit prohibition, the DMA lacks precise definitions for critical elements of the ban on self-preferencing, notably in clarifying what falls within the concept of

[233] Digital Markets Act, supra note 231, recital 32.
[234] *Supra* note 232, paragraph II, section A.
[235] Digital Markets Act, *supra* note 231, Art. 6(5).

discriminatory conditions. While it's relatively straightforward to discern discrimination in application (e.g., establishing different set of criteria for first-party versus third-party products), identifying and addressing discrimination by design—such as determining which parameters influence ranking and if they include a discriminatory bias — is considerably more challenging. [236]

While aforementioned precedents like the *Google Shopping* case have undoubtedly shaped the regulatory landscape, the DMA's self-preferencing prohibition in Article 6(5) DMA takes a more stringent stance by disallowing gatekeepers to argue on the basis of objective justification. Any economic discussion regarding the potential positive impacts of self-preferencing on competition and consumer welfare is precluded. [237] Other parts of the DMA address some of the types of conduct that may be considered self-preferencing in a broader sense. For example, Article 6(10) concerns equal access and use of data between first and third parties, to prevent more favourable treatment of first- versus third-party services, and Article 6(12) concerns fair, reasonable and non-discriminatory terms of access for a subset of core platform services.

Both the Commission and the majority of commentators interpret the DMA proposal as a primarily competition-oriented regulatory approach, which through its ex-ante per-se rule regime should make enforcement much more effective and faster than the traditional ex-post control of abusive behavior of dominant firms (Art. 102 TFEU). Others, on the other end, point out to the fact that this regulatory approach doesn't help to strengthen data protection and consumer protection vis-à-vis the economic power of gatekeepers.[238] Although the DMA wants to target the large tech firms with their digital platforms, "it does not take into account the intertwinement between competition and privacy problems, the implications of the simultaneous existence of the two market failure problems, and the interplay between competition-oriented rules and data protection and consumer protection rules", therefore, in the practical implementation of

[236] *Supra* note 232, paragraph III.
[237] *Id.*
[238] *Supra* note 13, at 293.

the DMA, "the Commission will have to deal with data protection and privacy issues as well as with typical consumer policy problems". [239]

In conclusion, the DMA's endeavours to address self-preferencing and promote equal treatment within core platforms service markets faces notable challenges, with a primary focus on the need to establish clearer criteria for detecting self-preferencing. Better guidance facilitates compliance and active monitoring, ultimately preventing circumvention. It is expected that additional guidance will emerge from proceedings following the implementation of the DMA, offering business users greater clarity on the extent to which they can enforce their rights under the provision. As the DMA aims to address the economic power of large tech firms while ostensibly focusing on competition, the real-world application and subsequent legal interpretations will reveal how effectively it navigates the complex interplay between ensuring competitive markets and protecting consumer privacy. Through this evolving landscape, we will gain valuable insights into the practical challenges and potential refinements needed to balance these dual objectives, ultimately informing both competition law and data protection policy in a digital era.

6. Conclusion

Digitization is profoundly reshaping our economies, societies, access to information, and ways of life. It has brought innovation, new products, and new services, embedding itself into the fabric of our daily life. However, its ubiquity has also sparked concerns about its political and societal impacts, and more pertinently, about the concentration of power among a few large digital firms. In Europe, competition law has come to play a special role in shaping both the public perception of the digital future, and the legal environment in which it is developing. Part of this role stems from its empirical focus and the thoroughness of the investigations by the competition authorities. The digitization of the economy—with the emergence of digital platforms and the key role of personal data for their business models—has led to the need of a deep change of the relationship between competition law and data protection (or privacy) law. This

[239] Kerber, *supra* note 13, at 294.

dissertation has explored the nuanced relationship between these two legal realms, particularly through the lens of digital platforms using privacy as a justification for anticompetitive conduct, effectively positioning themselves as *de facto* privacy regulators. The introduction of the Digital Markets Act (DMA) raises critical questions about its application to self-preferencing cases and the future interactions between competition law and privacy within this new ex-ante regulatory framework. The analysis of the two cases, Google Privacy Sandbox and Apple's App Tracking Transparency (ATT) policy, provides insights into the complexities of the economic power held by vertically integrated, data- driven, large dominant platforms. It underscores the necessity for a coordinated strategy that integrates competition, consumer protection, and privacy policies to address these challenges effectively. The latter cannot be resolved in isolation, but require a cohesive approach that involves cross-doctrinal cooperation between antitrust and data privacy enforcers. Such cooperation is essential to develop a robust and effective digital regulatory framework that can deliver benefits to the economy, consumers, and regulatory agencies alike and to ensure that the digital marketplace remains competitive and fair, protecting both consumer privacy and market integrity. This coordinated approach will be vital in harnessing the full potential of digital innovation while mitigating its risks. The intersection of the two areas of law represents a fertile ground for developing new theories and practices that can better navigate the challenges of the digital age.

BIBLIOGRAPHY

Academic Journals

1. Creser, Olivia T. "In Antitrust we Trust? Big Tech is Not the Problem - it's Weak Data Privacy Protections." *Federal Communications Law Journal* 73, no. 2 (2021): 289-316.
2. Geradin, Damien, Dimitrios Katsifis, and Theano Karanikioti. "Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective." *European Competition Journal* 17, no. 3 (2021): 617-681.
3. Höppner, Thomas and Philipp Westerhoff. "Privacy by Default, Abuse by Design: EU Competition Concerns About Apple's New App Tracking Policy" *Hausfeld Competition Bulletin,* (2021), Available at SSRN: https://ssrn.com/abstract=3853981 or http://dx.doi.org/10.2139/ssrn.3853981
4. Kerber, Wolfgang. "Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law." *Antitrust bulletin.* 67, no.2 (2022): 280–301.
5. Motta, Massimo. "Self-Preferencing and Foreclosure in Digital Markets: Theories of Harm for Abuse Cases." *International Journal of Industrial Organization* 90, (2023): 102974.
6. Peitz, Martin. "How to Apply the Self-Preferencing Prohibition in the DMA." *Journal of European competition law & practice* 14, no. 5 (2023): 310–315.
7. Reverdin, Vladya M. K. "Abuse of Dominance in Digital Markets: Can Amazon's Collection and use of Third-Party Sellers' Data Constitute an Abuse of a Dominant Position Under the Legal Standards Developed by the European Courts for Article 102 TFEU?" *Journal of European Competition Law & Practice* 12, no. 3 (2021): 181-199.
8. Thornhill, John. "Apple's Move To Increase Privacy Strengthens Its Walled Garden*." Financial Times* (March 18, 2021)
9. Wahyuningtyas, Sih Yuliana. "Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market." *European Business Organization Law Review* 18, no. 4 (2017): 785-800.

Reports and Acts of European, National Institutions and Authorities

1. AGCM, AGCom, Garante Privacy, Indagine conoscitiva *IC53 – Big Data* (Dec. 20, 2019), https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf
2. Competition & Markets Authority, *Online Platforms and Digital Advertising Market Study* (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
3. Competition and Markets Authority, case 50972, Q1 2024 update report on implementation of the Privacy Sandbox commitment, https://assets.publishing.service.gov.uk/media/662baa3efee48e2ee6b81eb1/1._CMA_Q1_2024_update_report_on_Google_Privacy_Sandbox_commitments.pdf
4. CMA, *Online Platforms and Digital Advertising market study, Appendix G: the role of tracking in digital advertising (2020)* [online] Accessible at: https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf
5. CMA, *Online Platforms and Digital Advertising market study, Appendix M: Intermediation in open display advertising* (2020) [online] Accessible at: https://assets.publishing.service.gov.uk/media/5efb22add3bf7f769c84e016/Appendix_M_-_intermediation_in_open_display_advertising.pdf
6. Commission Notice- Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, 2004/C 101/07.
7. Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Text with EEA relevance)(2009/C 45/02), art.19.
8. Conference of the Representatives of the Governments of the Member States, *Consolidated version of the Treaty on the Functioning of the European Union*, OJ L. 326/47-326/390; 26.10.2012, European Union, 26 October 2012.
9. Digital Competition Expert Panel, *Unlocking Digital Competition*, Furman Report (Mar., 2019); https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital- competition-expert-panel;

10. Douglas, Erika M., *Digital Crossroads: The Intersection of Competition Law and Data Privacy*, Annex 2 to the Report To The Global Privacy Assembly Digital Citizen and Consumer Working Group, (July 2021), http://dx.doi.org/10.2139/ssrn.3880737
11. European Commission, *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation* (June 24, 2020), https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN
12. European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., *Competition policy for the digital era*, Publications Office, 2019, https://data.europa.eu/doi/10.2763/407537
13. European Commission, Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
14. European Data Protector Supervisor, *Opinion 1/2021 on the proposal for a Digital Services Act* (Feb. 10, 2021). https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf
15. European Data Protector Supervisor, *Opinion 2/2021 on the proposal for a Digital Markets Act* (Feb. 10, 2021); https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf
16. EDPS, Preliminary Opinion, *Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (Mar. 2014), available at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf
17. Organisation for Economic Co-operation and Development (OECD), *Consumer Data Rights and Competition- Background Note* (2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.
18. OECD, Directorate for Fin. & Enter. Affairs Competition Comm., *Executive Summary of the Discussion on Quality Considerations in the Zero-Price Economy* -

Annex to the Summary Record of the 130th Meeting of the Competition Committee held on 27-28 November 2018 (2018), https://one.oecd.org/document/DAF/COMP/M(2018)2/ANN9/FINAL/en/pdf

19. OECD, Directorate for Fin. & Enter. Affairs Competition Comm., *Quality Considerations in Digital Zero-Price Markets – Background Note by the Secretariat* (Nov. 28, 2018), https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119, 4.5.2016, pp. 1–88.
21. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66;
22. Summary of Commission Decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39740 – Google Search (Shopping)).

Cases

1. AGCM Decision No. 30620 of May 2, 2023, Case A561 - Apple App Tracking Transparency Policy;
2. Competition and Markets Authority, 2022a. Case number 50972, 11 February 2022.

Online Sources

1. CompaniesMarketCap.com. (March 18, 2024). Leading tech companies worldwide 2024, by market capitalization (in billion U.S. dollars) [Graph]. In *Statista*. Retrieved March 23, 2024, from https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/