Industrial and Corporate Change, 2021, **00**, 1–24
DOI: https://doi.org/10.1093/icc/dtab053
Review

Regulating digital ecosystems: bridging the gap between competition policy and data protection

Beatriz Kira[1,*], Vikram Sinha[2] and Sharmadha Srinivasan[2]

[1]Blavatnik School of Government, University of Oxford, Oxford, OX2 6GG, UK. e-mail: beatriz.kira@bsg.ox.ac.uk and [2]IDFC Institute, 301, 3rd Floor, Construction House A 24th Road, Off Linking Rd, Khar West, Mumbai, Maharashtra 400052, India. e-mails: vikram.sinha@idfcinstitute.org; sharmadha.srinivasan@idfcinstitute.org

*Main author for correspondence.

Abstract

Data collection and processing are at the core of rapidly growing business models, underpinning the activities of technology companies and acting as a source of market power. The key role played by data in the competitive dynamics of digital ecosystems has brought competition policy and data protection regulation closer together and raised important questions about the substantive relationship between these two branches of law. After identifying the specific ways in which data create and power digital ecosystems and examining the effects of digital privacy (or lack thereof) on consumer welfare, we compare the legal obligations imposed by competition policy and data protection regulation. We then map the interfaces between these two branches of law and critically assess the areas of substantive overlap between them. We show that while in the majority of situations there is an alignment of these two frameworks, opposite outcomes can sometimes be reached when competition and data protection rules are applied separately. We suggest that these two legal instruments should be considered as overlapping areas in a regulatory continuum to facilitate positive synergies and neutralize potential conflicts. We show that there is a significant scope for competition policy actors and institutions to substantially incorporate data protection considerations into their decisional practice and that this integration can inform and enhance the enforcement of competition law. We propose an integrated approach to more effectively regulate digital platform ecosystems, to support innovation, and to protect consumers and the competitive process.

JEL classification: K21, K23, D42, D43, L86

1. Introduction

Over the past few years, technology companies have grown to become some of the largest firms in the world. Google, Apple, Amazon, and Microsoft each have a market value of more than US$1 trillion. While these companies have undoubtedly contributed to the creation of a wide range of innovative and efficient products and services, their business models have also given rise to complex and interconnected policy issues.[1] A series of expert reports and studies have analyzed

1 The term 'business model' in this article is generally used to describe the rules, roles, strategies, and relationships that are characteristic of a given sector and corresponds to what Jacobides *et al.* (2006) call 'industry architecture'. When referring to the wider set of interconnected roles and relationships at play in digital ecosystems and the monetizing strategies employed by them, the term 'business model' corresponds to what Jacobides and Lianos (2021) call 'ecosystem architecture'. For a review of the specialized literature on the concept of business models, see Zott *et al.* (2011), and on the importance of working with business models to design regulation, see Caffarra *et al.* (2020).

competitive dynamics in markets dominated by technology companies.[2] Despite differences in the scope of these reviews and their recommendations, there is a growing consensus that competition is *not* one click away, and the rules and tools that have regulated analog markets need to change to be fit for purpose in the digital age.

There is broad agreement that different forms of regulation, beyond the conventional competition law framework conceived for brick-and-mortar markets, are needed to address the risks posed by digital ecosystems Traditional competition law is often inadequate or insufficient to deal with competition issues in digital markets (Jenny, 2021). From the lack of appropriate tools for identifying power and dominance in ecosystems and the limitations of *ex post* competition frameworks to address issues related to dynamic competition (Jacobides and Lianos, 2021), to the emergence of data issues in connection with competition law (Jenny, 2021), the functioning of digital markets has raised profound questions about the fitness of competition law and its underpinning theories. The overarching question is not only about the need to adopt new rules or to change the interpretation of existing ones but also whether to revisit the principles upon which competition law is founded (Biggar and Heimler, 2021) and whether a more holistic approach to competition law is required to accommodate all dimensions of ecosystem competition.

Data protection and privacy regulation have gained particular attention in current debates around suitable frameworks to supervise digital platform ecosystems Whether for protecting individual rights, for economic regulation of data controllers, or a combination of both, specific regulatory models were adopted in different jurisdictions establishing rules for the protection of personal data and their associated rights.[3] Data protection regulations usually establish the right to access, deletion, and portability of data, and procedures to mitigate risks and protect individuals against threats that could arise from data processing activities.[4] A flagship piece of legislation is the European Union (EU) General Data Protection Regulation (GDPR), which entered into force in 2018 and is fast becoming a global standard for 'best practice' in data governance (Bradford, 2020; Greenleaf, 2021).[5] The protection of privacy as a fundamental right has also gained prominence with the emergence of new surveillance technologies (Zuboff, 2019; Véliz, 2020). While from a legal perspective the right to privacy is often framed as the 'right to be let alone' (Warren and Brandeis, 1890), from a market perspective, privacy has been put on a commercial footing, with some economists framing it as a commodity traded in data markets (Economides and Lianos, 2021).

Although data protection and competition law originate from different social concerns and specific legal tenets and methodologies, the emergence of digital markets and the role played by data driving the business models of technology firms (Caffarra *et al.*, 2020; Jacobides *et al.*, 2020) have brought these two fields closer together. On the one hand, there are concerns that the growing market power of technology companies that control the nature and volume of data collected and processed across digital ecosystems could translate into a systematic impediment to individual rights. On the other hand, data collection and processing have upended revenue models and marketplace functioning, making access to data an important source of market power. Crucially, the existence of zero-price platform-based ecosystems such as Facebook and

2 For example, Furman *et al.* (2019) discuss the UK scenario. Scott Morton *et al.* (2019) focus on the United States, as does the US House Judiciary Committee report (2020). Crémer *et al.* (2019) discuss similar issues in the context of the EU. Lianos and Ivanov (2019) examine digital competition in the BRICS countries (Brazil, Russia, India, China, and South Africa). See Lancieri and Sakowski (2020) for a comprehensive review of reports and studies on topics related to competition in digital markets.

3 The normative foundations of data protection and privacy legislation vary across jurisdictions, and different regulatory models and institutional designs have been adopted to implement it. For example, the EU Charter of Fundamental Rights sets out a right to data protection, which is independent of the established right to privacy (González Fuster, 2014). In the United States, data protection regulation is fragmented, composed of a patchwork of sectoral, federal, and state laws and complemented by a self-regulatory regime. While there is no national data protection regulator, the Federal Trade Commission has been performing the activities of a data protection authority at the federal level and led the development of a jurisprudence on information privacy in the United States (Solove and Hartzog, 2014).

4 Around the world, 145 countries have adopted data protection laws, and over the past 5 years (2017–2021), another 23 nations have official bills in various stages of progress for the introduction of similar legislation (Greenleaf, 2021).

5 The global influence of the GDPR can also be explained by countries' ambition to be able to consider applying for 'adequate' status under the EU's GDPR, which would allow the unrestricted flow of data between their territories and the EU and facilitate access to the European common market. See Greenleaf (2021).

Google is made possible by the means to monetize data. While the term 'free' describes the absence of a monetary price charged to the final consumer, the data harvested by the platform can represent nonmonetary costs charged to users in exchange for the free services and products (e.g. social networking or email), as we explain in Section 2.2. This creates regulatory concerns that have proved stubbornly resistant to monocentric competition policy focused on price.

Despite calls for a more substantive alignment of data protection and competition law (Lynskey, 2018), the antitrust literature has not yet explored the interface between the two fields systematically and has framed the debate as *either* a matter of improving antitrust mechanisms *or* adopting a new regulatory framework. The recent ruling by Germany's Federal Court of Justice, which backed the decision made by the competition authority in a flagship case involving Facebook, can be considered a precedent for a more integrated approach.[6] However, there is no clear analytical framing yet of the relationship between data protection and competition law when it comes to digital ecosystems This article aims to address this gap by suggesting a practical analytical framework that encompasses both fields.

The current compartmentalized approach means that potentially beneficial synergies are often overlooked. More concerning, on the exceptional occasions where their objectives conflict, applying competition law and data protection regulation separately can lead to distinct outcomes. Anecdotal evidence indicates that while limits to data collection and processing can enhance users' privacy, they can also entrench data advantages and favor the business model of large platforms over small- and medium-sized enterprises (SMEs), leading to less competitive markets. Access to databases and efficient data processing can contribute to cost reductions in production and improved quality of digital goods and services. Lack of sufficient data might prevent companies from building a database that can help to offer goods and services at a competitive level. More specifically, the cost of complying with strict data protection laws, such as the EU GDPR, can make it more difficult for companies to enter the market, entrenching the power of incumbent companies and harming competition (Furman *et al.*, 2019).

We propose a new framing for examining the relationship between competition law and data protection regulation. By looking at their common boundaries and mapping the interfaces between the two frameworks, we demonstrate how a more holistic and integrated approach can facilitate positive synergies and neutralize conflicts, leading to a more effective supervision of digital ecosystems[7] More broadly, an integrated framework is essential for developing what Lianos (2018) dubbed 'polycentric competition'—a multidimensional policy approach to consumer preferences and welfare in dynamic, evolving digital markets where monetary price levels are a two-dimensional, inaccurate proxy for complex consumer preferences. We argue that the boundary between competition law and data protection regulation is not as clearly defined as the literature implies. Rather, these two instruments should be considered as areas in a regulatory continuum with a large area of overlap.

The article is structured as follows: Section 2 maps the specific ways in which digital platforms and ecosystems rely on data to establish and consolidate market power and the implications of digital privacy (or lack thereof) for consumer welfare; Section 3 describes the analytical framework, examining the points of convergence and divergence between competition policy and data protection, with examples of relevant intersections; Section 4 proposes ways to reconcile the two frameworks by integrating data protection considerations into competition policy analysis; and, finally, the conclusion summarizes the arguments and highlights how this article adds to the literature on digital markets.

6 See Bundesgerichtshof KVR 69/19, 23 June 2020, and Bundeskartellamt B6-22/16, 6 February 2019.

7 The framework proposed here is not focused on any specific country, but it assumes the coexistence of data protection rules and robust competition policy. This underlying assumption certainly restricts the universe of countries the framework applies to. However, for jurisdictions where one or both regimes are not yet implemented, the article is also relevant, as it calls attention to the risks emerging from the regulatory gap and highlights the role of these rules in the regulation of digital platforms.

2. Understanding the role of data in digital ecosystems

Over the past two decades, a wide body of literature has discussed digital platform markets, focusing on network effects and high switching costs. More recently, economists and legal scholars have focused on the challenges of enforcing antitrust legislation in digital platform ecosystems, examining the ways data plays a role in competition dynamics. Despite the lack of a shared definition and clear understanding of the nature of these markets, there is a growing consensus that their structure and functions pose new challenges that demand some sort of regulatory intervention (Jacobides and Lianos, 2021).[8]

2.1 Data as a source of market power

Digital platforms generally operate in multisided markets where users in each market 'directly interact with each other facilitated and observed by the platform operator' (Martens, 2016). These platforms benefit from direct network effects among users on one side of a platform and indirect network effects stemming from cross-platform complementarity (Evans and Schmalensee, 2016). Digital platforms also have distinct supply-side economies of scale, with high fixed costs for initial investment, but low marginal costs. This can create a positive 'feedback loop': more sales means lower unit costs and a greater value proposition for new customers (DeLong and Froomkin, 2000; Varian *et al.*, 2004). Therefore, users tend to converge on a particular platform in a 'winner takes all' phenomenon (Galbraith, 1995) where network effects combined with increasing returns can 'tip' the market in favor of a dominant firm.

The data that fuel digital platforms heighten these dynamics in a way that is qualitatively and quantitatively different from conventional markets. A traditional firm can only collect data on its own customers, but a digital platform can access a vast amount of data related to all sellers and buyers on multiple sides of its platform (Eisenmann *et al.*, 2011). Digital platforms are able to capture large volumes of information about users from many different sources. The volume, velocity, and variety of these harvested data—the so-called '3 Vs'—enable 'data network effects' (Bundeskartellamt, 2016). These function similarly to traditional network effects: more users contribute to more data generation, which helps to improve services and products, in turn leading to better user targeting and services (Turck, 2016). As a result, market checks on producer surplus (Varian *et al.*, 2004)—intense competition to retain monopolies, and leapfrogging established platforms with radical innovation—become increasingly unlikely.

Different platforms collect and monetize data in various ways: either through a direct subscription model (e.g. Spotify)—by using collected data to tailor products directly to users (e.g. Amazon)—or by selling targeted ads (e.g. Facebook and Google Search). Most zero-price ad-based platforms use the latter business model, enabling them to establish market power in the complementary positive-price digital advertising market. These platforms can also realize a greater value from the data they have collected by merging data sets. This allows them to generate inferences about consumer preferences, behavior, and social networks (among other information) that they can leverage in adjacent markets (Stucke and Grunes, 2016). More broadly, it enables platforms to establish market power across the whole supply chain and ecosystem complementors (Jacobides *et al.*, 2019). The dominant players that fashion these ecosystems have access to many complementary users (e.g. search users and advertisers for Facebook) or offer complementary products (e.g. Apple music, iPods and Apple TV for Apple), and so are able to leverage their central position within the ecosystem. This is not limited to entrenching their central position by limiting competition within the ecosystem; they also lock in users and raise the costs of switching to an alternative ecosystem (Jacobides and Lianos, 2021).

The traditional antitrust toolkit is unable to effectively address such data-fueled anticompetitive behavior. Competition law, with its methodological focus on the relevant product market, is unable to capture the complex dynamics of platforms asserting their market power in the ecosystem of various complementary products (Jacobides and Lianos, 2021). For example, Alphabet,

8 Some authors argue that regulatory intervention should encompass not only state regulation but also at least some level of self-regulation, whereby a company or an association of firms develops and implements commands and consequences on itself (see Cusumano *et al.*, 2021).

with its Android operating system, can dictate terms in the app development and content markets but also to related market players upstream such as handset and mobile device manufacturers (Morton and Dinielli, 2020). Competition authorities are starting to take notice of this dynamic. For example, in June 2021, the European Commission (EC) and the UK's Competition and Markets Authority (CMA) opened investigations into Facebook's use of advertising data and whether this gave the company an unfair advantage over competitors, allowing it to benefit its own services such as Facebook Marketplace.[9]

2.2 Data and consumer welfare

From an antitrust perspective, data collection and processing also have implications for consumer welfare. Despite differences at philosophical, political, legislative, and enforcement levels, consumer welfare is part of the core of competition policy that is shared by different jurisdictions. According to Ezrachi (2017, p. 51), 'while competition laws around the world differ in language, provisions, and interpretation, they reflect large degrees of consensus on what competition law is set to achieve'. For instance, the United States has focused on this economic goal to the exclusion of others (Stucke, 2012). Notwithstanding judicial and academic skepticism, the EU also converged with this standard, following the Economic Advisory Group on Competition Policy's discussion paper (2005); (Wils, 2014; Ibáñez Colomo, 2016).

Consumer welfare from an allocative efficiency perspective remains the cornerstone of competition regulation (Hovenkamp, 2020).[10] Assessing consumer welfare in allocative efficiency terms in positive-price digital platform markets is no different than in traditional markets: monetary transactions function as market-signaling costs on the consumer side of digital platforms, as they do in conventional markets. However, both the conventional and the 'thick' concepts of consumer welfare defended by neo-Brandesians (Khan, 2017)—the understanding that a price focus leads to delayed, ineffective *ex post* regulatory action—become considerably more complicated in zero-price digital platform markets.

In these markets, according to Evans (2011), a 'vast amount of consumer surplus […] likely results from products and services offered for free'. Zero-price is not a predatory pricing tactic to be followed by recoupment; it is the long-term equilibrium price. Brynjolfsson and Collis (2019) develop a framework for capturing the benefits of such products and services using incentive-compatible discrete choice experiments. They show considerable gains in consumer welfare and gross domestic product from popular digital goods such as Facebook, Twitter, Instagram, and Skype, among others. Brynjolfsson *et al.* (2019) build on this, demonstrating that choice experiments can be used to estimate reservation prices that can give households benefits of using zero-price products.

The flip side of this is that these advertising-driven zero-price platforms, including social messaging and online search, are functional markets where consumer welfare and the competitive process can also suffer.

2.2.1 Data as nonmonetary costs

Data can be considered a medium of commercial and economic exchange. Even though the 'value of data' is hard to quantify using traditional metrics, there is a growing realization of its role in economic transactions (Brynjolfsson and Collis, 2019). Other regulatory realms have recognized this: contract law is a good example. Indian contract law links the definition of price to consideration, which is a promise of an exchange of value (Jatania, 2019). Jurisprudential precedent establishes a similar logic in the United States. In *Gottlieb v. Tropicana Hotel and Casino*,[11] the court recognized that 'the information cost functioned as consideration—it signalled the presence

9 See the press releases by the EC and the CMA: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2848 and https://www.gov.uk/government/news/cma-investigates-facebook-s-use-of-ad-data; accessed June 6 2021.

10 Some scholars have argued that, in the face of digital markets' challenges and the large size of technology companies, competition policy should move away from the consumer welfare standard entirely and target economic concentration instead. However, discussing perspectives such as neo-Brandesian structuralism or other scholarship, such as the Chicago School of antitrust, is beyond the scope of this article.

11 See Gottlieb v Tropicano Hotel & Casino, 109 F. Supp. 2d 324, 327 (E.D. Pa. 2000).

of a bargained-for exchange. The fact that Ms. Gottlieb exchanged her personal information instead of money was of no moment' (Newman, 2015).

Antitrust literature and regulatory policy have applied similar logic in recent years. Essentially, consumers pay for a product or service with their data (Hoofnagle and Whittington, 2014; Malgieri and Custers, 2018). Newman's (2015) taxonomy of costs in zero-price markets divides cross-platform consumer–supplier interactions into nonmarket-signaling costs (unilateral opportunity costs and external costs borne by a third party) and market-signaling attention and informational costs. As Newman (2015) puts it: 'When the benefits offered exceed the total costs to the customer – including the costs of surrendering the information sought – a rational customer will surrender the requested information'. By acting on the supply curve, information costs replicate the monetary function of revealing consumer preference in a commercial exchange.

In India, a Competition Law Review Committee (CLRC)—established to recommend amendments to the country's Competition Act to better enable the country's competition authority to regulate digital markets—has come to a similar conclusion. Its 2019 report considered whether the definition of price in the Competition Act should be amended to specifically include data. It concluded that this was unnecessary because the current definition of price encompasses 'every valuable consideration, whether direct or indirect' and is wide enough to encompass any kind of consideration that has a bearing on a service or product (CLRC, 2019).

Framing nonmonetary data costs in this manner has clear implications for exploitative conduct in the form of overcharging. For example, platforms such as Google and Facebook can overcharge end users through default opt-in models that allow them to harvest more information. These 'exploitative data practices' point to a market failure in digital markets where users are faced with a restrictive choice of either not using the platform or accepting their terms (Economides and Lianos, 2021).[12] Especially in cases where the digital platform is central to the ecosystem, its ability to dominate the ecosystem and exert power in complementary adjacent markets may rest on these exploitative data practices (Jacobides and Lianos, 2021) (we explore this in Section 3.1).

2.2.2 Data protection as a dimension of product quality

Competition on quality in conventional positive-price markets is often folded into competition on price (Evans, 2011). The objective, standard value of price allows regulators to treat it as a measure of consumers' revealed preference for products after accounting for quality. Assessing users' preferences and the quality of goods and services in digital markets is more complex. Digital platform models often use dynamic pricing that factors in cross-platform effects—for instance, the 'price surge' mechanism in ride-hailing services. In economic terms, cross-subsidization and indirect network effects mean that product quality in Market A on one side of the platform may be affected by Market B on the other side without changes in prices in Market A.

Zero-price platform models multiply the difficulties given the absence of the standard metric of price. Some have suggested that quality should be treated as a standalone competition metric in such markets—a 'small but significant nontransitory decrease in quality' metric (Waehrer, 2016; Crémer *et al.*, 2019). This assessment would consider the scope of data collection to the extent that it affects consumer privacy as a measure of product quality (OECD, 2018). Such degradation in quality can be seen in search engines, which have an incentive to prioritize data collection and search results for generating more pay-per-click ad revenue rather than for providing the most relevant search results (Ezrachi and Stucke, 2015), (as we explore in Section 3.4).

3. The intersection of competition policy and data protection

The previous section analyzed the practical and theoretical challenges of digital platform business models, with particular attention to the role of data. These challenges give rise to different

12 Economides and Lianos (2021) argue that this market failure could be resolved by a 'missing market' for data where companies could buy personal data, allowing consumers to reveal their preferences for privacy and control over personal data. However, this would be complicated in some jurisdictions by a 'rights' approach to privacy, which may place restrictions on the use of personal data even when consent has been taken.

Table 1. Relationship between data protection and competition

	Positive competitive outcomes	Negative competitive outcomes
Positive data protection outcomes	Companies compete on data protection, and the extent to which companies protect users' data can be a competitive advantage. There are incentives for companies to invest in products and policies that offer greater levels of protection to users' data (e.g. privacy by design)	Lack of data can prevent companies from building a critical database or from offering goods and services at competitive levels. This makes these companies less likely to survive in data-driven markets, leading to a decrease in competition
Negative data protection outcomes	In competitive markets, companies compete fiercely for data, employing invasive techniques to gather large amounts of users' data. However, this information can be used to improve the quality and efficiency of goods and services, leading to a drop in costs	Intrusive data collection techniques might lead to data concentration. Data monopolies have fewer incentives to compete on privacy and are able to use market power in new anticompetitive ways. Data concentration can also increase the risks of surveillance and security breaches

levels of interaction between competition policy and data protection rules. This section maps out the points of intersection between the frameworks for data protection and competition (as summarized in Table 1) and discusses why they deserve greater scrutiny.

Some analyses have pointed to the divergences seen in Table 1 as evidence of the lack of compatibility between competition and data protection regimes—particularly in the context of the GDPR (Gal and Aviv, 2020). However, there are two reasons why this is merely an operational conflict, not a normative one. Firstly, compliance costs that may advantage larger companies, which have greater capital and structural capability to bear the burden, are a potential pitfall of all regulatory regimes, not just data protection. This can be mitigated by assessing trade-offs and calibrating the regulatory framework effectively. Secondly, overlapping regulatory regimes that are developed in parallel may come into conflict at times (EDPS, 2014). This apparent conflict highlights the need for a more holistic approach to drafting regulatory frameworks.

In most situations where these regimes overlap, competition policy and data protection can be regarded as complementary because their objectives are substantially similar. In these cases, either by preventing a negative outcome in both areas or by fostering positive synergies between them, an integrated regulatory approach can benefit consumers. However, in some situations, the concurrent enforcement of these rules to frame a given behavior or to review the effects of a proposed merger can lead to divergent outcomes. Cases considered legitimate by competition policy may be deemed unlawful when the data protection framework is applied. Equally, a situation that is considered legitimate under data protection provisions could violate competition law. Therefore, in the cases highlighted in the top right and bottom left quadrants in Table 1, our proposed integrated approach is even more important to prevent divergences in outcomes from the fragmented application of different criteria to the same set of facts.

3.1 Negative competitive outcomes overlap with negative data protection outcomes

The dynamics of monopolization and lack of data protection can be self-enforcing. When big tech companies act as digital gatekeepers, only a handful of players have access to the data needed to thrive in digital markets. Digital gatekeepers are not merely defined by their size or market power but can be broadly defined as those that act as an unavoidable interface between businesses and customers (Jacobides *et al.*, 2020; Geradin, 2021). They hold a significant amount of power in the online ecosystem, especially over access to key infrastructure. The proposed EU Digital Markets Act (DMA), for example, defines gatekeepers as enjoying an 'entrenched and durable' position in the market in addition to also specifying quantitative metrics of number of users and market turnover (Jacobides and Lianos, 2021).

Data concentration makes it harder for more efficient entrants to displace an incumbent, as new players would have difficulty gathering a large enough critical mass to enter the market

(Evans, 2003; Stucke and Grunes, 2016). In the absence of data regulation that specifies the situations where data can be shared, incumbents would not have incentives to provide access to key data that would enable new players to enter markets. The lack of rules and procedures to allow users to access their own data held by technology companies and to ensure data portability might prevent complementary businesses and potential competitors from having access to key data sets. This would raise switching costs and favor incumbents.

Despite the growth in the adoption of data protection measures and privacy-by-design in product development, technology companies still have strong economic incentives to employ powerful data collection and intrusive data processing tools. In the absence of data protection laws, companies would adopt lower privacy settings as default—allowing, for example, the processing of data without explicit consent. From an antitrust perspective, such excessive data collection by companies could be considered abuse of dominance, comparable to excessive pricing under European competition law (Costa-Cabral and Lynskey, 2017; Robertson, 2020).

Collection of data through the 'default opt-in' option can also be seen as a market failure and a default opt-out could reduce excessive data collection (Economides and Lianos, 2021). For example, the Bundeskartellamt (Germany's competition authority) found that Facebook's terms and conditions violated data protection and competition rules, arguing that they are 'neither justified under data protection principles nor are they appropriate under competition law standards'.[13]

At the same time, weak competition and concentrated market power may lead to reduced levels of data protection (Kerber, 2016). Consumers' privacy choices are limited in less competitive markets that are dominated by a few players. Their privacy preferences are likely to be better served in a market with several players (Esayas, 2018a). Where a few companies have dominance, they have little incentive to compete on data privacy and are more likely to engage in excessive data collection and offer less privacy protection than in a competitive market. Strong network effects and high switching costs would prevent users from looking for more privacy-friendly alternative platforms (Condorelli and Padilla, 2020). With fewer options to switch to, digital platforms could also collect more data and compensate users less than they would in a competitive market (Economides and Lianos, 2021).

In data-driven markets, abuse of dominance takes place in new ways. The employment of highly tailored and segmented profiling technologies, such as microtargeting or geotagging, can enable a platform to restrict competition and prevent users' access to certain goods or services based on their personal features. For example, in 2017, the EC launched an investigation to assess if certain video game companies were preventing consumers from having access to digital content based on their location or country of residence.[14] This would be considered a geo-blocking practice, which uses consumers' data to prevent them from enjoying cross-border choice and being able to buy computer games at competitive prices.

According to a structuralist approach, platforms in direct competition with businesses that depend on them hold a privileged position for influencing the way the industry is structured and the value allocation between the industry players. Many of the biggest digital platforms are integrated across business lines so they operate and market their own goods and services on the same platform (e.g. Amazon and Google). As a result, such platforms have the means and incentives to exploit their structure to further entrench their dominance (Wu, 2018; Khan, 2019; Lianos, 2019).[15]

13 See decision press release by Bundeskartellamt (7 February 2019). https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5; accessed 14 July 2021.

14 EC Press release, 'Antitrust: Commission sends Statements of Objections to Valve and five videogame publishers on "geo-blocking" of PC video games' (IP/19/20105, 5 April 2019).

15 Khan (2019) proposes a framework to identify 'dominant platforms', which hold market power and are able to thwart competition and stifle innovation. According to the scholar, 'relevant factors could include: (1) the extent to which the entity serves as a central exchange or marketplace for the transaction of goods and services, including the level of market power that it enjoys in its platform market; (2) the extent to which the entity is essential for downstream productive uses, and whether downstream users have access to viable substitutes for the entity's services; (3) the extent to which the entity derives value from network effects, and the type of network effects at play; (4) the extent to which the entity serves as infrastructure for customizable applications by independent parties; and (5) the size, scope, scale, and interconnection of the company'.

Increased market power allows firms to be more opaque about how they use the data they collect. For positive-price platforms, while the main revenue model may rest on subscriptions or the goods purchased from a seller (e.g. Netflix or Amazon retail), additional customer data are used to target marketing based on past purchasing returns, which gives a competitive advantage. Amazon, for example, reportedly uses data of third-party sellers to better pitch its own products as well as test new products and foreclose competition (Khan, 2017).

With digital platforms that function as data monopolies, there is also a risk of greater surveillance and data leakages. When a small number of firms control a large amount of data, it is easier for governments to target them and gain access to the stored data, either by formal legal requests or through government hacking.[16] For example, the use of contact tracing apps by governments in response to coronavirus-19 triggered a debate about the potential use of the large amounts of data collected in the aftermath of the pandemic (Tisné, 2020). Likewise, security breaches by ill-intentioned agents would expose a much greater amount of information when data are concentrated in the hands of a few companies (Stucke, 2018).

If data are to be treated as a nonmonetary cost (as discussed in Section 2.2.1), it is possible to apply the logic of overcharging in positive-price markets—that is, when a supplier's dominant market position allows it to impose costs that do not accurately reveal consumer preferences and valuation of the product. Kemp (2020) traces data overcharging to 'concealed data practices'. The author argues that zero-price platforms suffer from deep information asymmetry regarding data transactions, with consumers unaware of the true scope of data extraction, the nature and scope of the data's use, and the consequences. These issues of privacy and consent do matter to individuals despite literature on the 'privacy paradox'—whereby users tend not to care about their privacy as much as they state and as revealed through their actual behavior (Barnes, 2006). As Solove (2021) points out, the privacy paradox is based on faulty assumptions where people's privacy concerns are general in nature and cannot be assessed in very specific contexts.

Further, privacy policies framed by companies may downplay risks, and the lock-in effect of certain platforms may affect consumers' actions regarding privacy (Reyna, 2018). This calls for regulation to be focused on how information is used and shared. However, despite the changes to terms of service influenced by data protection regulations such as the GDPR, this asymmetry persists, allowing suppliers to impose data 'costs' that are more than what consumers agreed to—or thought they agreed to. Enhanced consent mechanisms in the GDPR do not solve this problem. Information asymmetry perseveres because it is impossible in a modern platform market to reveal the full scope of data practices in a way that consumers can fully comprehend (Solove, 2012).

The inferential potential of personal data increases information asymmetry. As well as not knowing the full extent of data they are surrendering through terms of service, online tracking and other data processing practices, consumers are also unaware of the inferences about their lives that can be generated from the data they have willingly exchanged for a product or service (Solove, 2012; Hoofnagle and Whittington, 2014; Scott Morton *et al.*, 2019; Wachter and Mittelstadt, 2019; Kemp, 2020). This inferred information may reveal characteristics or preferences that consumers wish to conceal. It may also expose consumers to multiple objective harms such as increased 'attack surface' for digital malfeasance and discrimination (Kemp, 2020).[17]

16 For an overview of how governments hack computer systems for law enforcement purposes and how federal law regulates government malware in the United States, see Mayer, 2018.

17 There is the argument, however, that current data protection laws around the world are unfit to protect relevant collective aspects emerging from the business models of digital technologies, such as inferred harms and other collective harms with externalities on society at large (e.g. non-users, minorities, and anyone who is not on the system). Big tech companies extract most value from processing collective data, and so, as long as the focus of data protection rules is on the protection of individual rights and the individualization of data rights, relevant data-driven harms would go unredressed (Tisné, 2020). India's Ministry of Electronics and Information Technology (MeitY, 2020) attempted to address this with its expert committee report on a governance framework for non-personal data (MeitY, 2020), but this is an initial attempt with the framework's effects on both data protection and competition yet to be examined fully.

3.2 Positive competitive outcomes overlap with positive data protection outcomes

Companies may exert and entrench market power by reducing the level of data privacy, leading to negative outcomes according to both frameworks. The flip side of the argument is also true: dominant firms are more able to sustain data-invasive practices, so more competition can lead to better privacy protection. A competitive market might also lead to the deployment of privacy-enhancing technologies (PETs), as firms engage in 'competition on data protection', offering consumers products that give a higher level of privacy and data protection (Costa-Cabral and Lynskey, 2017; Esayas, 2018a).

When users have a better understanding of the risks involved in sharing their personal information online, they value services and devices that show more commitment to their privacy (Reyna, 2018). Enhanced privacy awareness creates incentives for companies to invest in products and policies that offer greater levels of protection to users' data. Many companies have now acknowledged that privacy can be a competitive advantage and are competing through data protection and differentiation. For example, the search engine DuckDuckGo promises users that it does not track or share their personal data, thus differentiating itself from other search services.

Emerging empirical evidence provides evidence of a relationship between the number of players in a market and competition through data privacy. Based on the data collection practices of 140 websites, Preibusch and Bonneau (2013) found that a sizable proportion of online consumers considers differences in data collection and processing when choosing between alternative suppliers. Significantly, they found that 'web sites which do not face strong competition are significantly more likely to ask for more personal information than other services provided for free, such as Web search or blogging' (Preibusch and Bonneau, 2013).

Antitrust authorities also increasingly recognize that companies can compete on privacy and data protection and that the level of data protection and privacy offered by a product or service could be subject to antitrust analysis as an element of quality, choice, or innovation (EDPS, 2014; Lynskey, 2018; Esayas, 2018b). In the Microsoft/LinkedIn merger case, the EC recognized that data privacy is 'a significant factor of quality' and, therefore, should be considered as a parameter that companies can either compete on or stifle competition.[18] Similarly, the EC investigation into Apple's takeover of song-recognition app Shazam also examined whether the merger would lead to further concentration of 'commercially sensitive data about customers'—but later decided it would not significantly impede effective competition in any of the identified relevant markets.[19] However, this ruling remains pertinent because it clearly articulated the concentration of data as a potential competition concern.

Costa-Cabral and Lynskey (2017) argue that the relevance of data for companies providing zero-price products goes beyond its use for the complementary advertising market. Its value for innovation and new market entry means that data acquisition should be treated as a distinct market where suppliers may compete on privacy—and the failure to do so feeds into the problem of missing markets referred to in Section 2.2.1. The EC's ruling in the Facebook/WhatsApp merger case bore this out. It acknowledged the existence of competition on privacy as a component of overall user experience or product quality and pointed out that many communication apps specifically addressed privacy issues.[20]

Data portability rights, such as the one included in the GDPR, could empower individuals in terms of control over their data. These rights could also favor competition between digital platforms by allowing users to multihome (to sign up to multiple competing platforms) more easily. This would reduce switching costs and lower barriers to entry, fostering a more competitive market. However, data portability alone may not reduce entry barriers. Smaller firms would have to deal with greater compliance costs to ensure data portability by design. It might also make it

18 EC Press release, 'Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions' (IP/16/4284, 6 December 2016). https://www.europeansources.info/record/mergers-commission-approves-acquisition-of-linkedin-by-microsoft-subject-to-conditions; accessed 14 July 2021.

19 See Case M.8788—Apple/Shazam. https://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf; accessed 14 July 2021.

20 See Case M.7217—Facebook/WhatsApp. https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf; accessed 14 July 2021.

easier for incumbent firms to collect data through other platforms—especially where the adopted standards are those of the incumbent firms (Cowen, 2018; Borghi, 2019).

3.3 Positive competitive outcomes overlap with negative data protection outcomes

In some circumstances, poor privacy outcomes can be associated with competitive markets and with more innovative and efficient products. An increase in the level of competition could, in some cases, have negative effects on data protection.

Competition could arguably promote more intense efforts to obtain users' details and lead to consumers having less control over their personal data. Companies compete by introducing new features that solicit more data from users. Casadesus-Masanell and Hervas-Drane (2015) empirically show that even though consumers disclose less information under competition than under monopoly, 'higher intensity of competition between firms [..] can increase the stock of information disclosed, reducing consumer privacy'. The increased amount of data about user preferences and characteristics is crucial for creating content that is better tailored to people's interests and the development of more efficient products and services. Therefore, information harvested by internet companies can contribute to reducing the cost of production and improving quality in such markets.

Some of the regulatory proposals to address digital platforms' competition challenges include mandatory data-sharing obligations for dominant players (Furman *et al.*, 2019). However, in the absence of robust data protection rules, such schemes might favor economic efficiency reasons, which are often at odds with the goals of data protection regulation (Graef *et al.*, 2018). Although granting competitors access to the data accumulated by a dominant platform might help to eliminate entry barriers, it could also be problematic for data protection due to the further sharing of private data (Kerber, 2016). Competition enforcement in the absence of comprehensive data protection regulations might risk turning 'one privacy offender monopolist into several privacy offender competitors' (Kimmelman *et al.*, 2018). Competition might also trigger a 'race to the bottom' and make it more difficult to enforce existing data protection rules, as multiple smaller firms could be more difficult to regulate than a few large ones (Shapiro, 2019).

Data-sharing requirements might also conflict with data protection rules. While providing access to a competitor's data could lower market entry barriers, it could be problematic if not designed to comply with general principles of personal data protection (Graef *et al.*, 2019; Tombal, 2021). A particular clash emerges under EU competition law, where there is a relevant discussion on the application of the essential facilities doctrine to personal data, whereby an incumbent company can be required to share data if '(i) it holds a dominant position on the relevant market and (ii) the refusal to give access amounts to an abuse of that dominant position', based on article 102 of the Treaty on the Functioning of the European Union (Graef *et al.*, 2018). In those cases, the incumbent firm can argue that an obligation to share data clashes with data protection rules, in particular those prohibiting sharing data with third parties.

3.4 Negative competitive outcomes overlap with positive data protection outcomes

This is perhaps the most complex interaction between the two regimes, because it often stems from the 'competition on privacy' detailed in Section 3.2—or an ersatz version—but has very different outcomes. It is also arguably the most relevant, given the ongoing attempts by dominant companies such as Apple and Google to enhance their leverage and competitive advantage over complementors and rivals under the guise of enhancing consumers' privacy. Because data collection and processing determine which companies can compete and thrive in digital markets, an increment in the level of data protection can lead to a decrease in competition. Apple and Google are creating a template for how to 'weaponize' such data protection to block other companies' access to data, thereby preventing them from building a critical database or from offering goods and services at a competitive level. Consequently, these other companies might not be able to survive, leading to even less-competitive markets.

Apple's recent iOS 14 policy changes exemplify this. The company has increasingly been positioning its mobile ecosystem as the 'privacy conscious' option, protecting consumers from violations of their digital privacy. This is a legitimate and potentially beneficial strategy to catalyze competition and innovation in consumer privacy. However, while it is a privacy-enhancing move, the iOS update is also a targeted attack against complementors in its ecosystem—businesses that sell products or services that add value for Apple's customers. While Apple has made it considerably harder for third-party apps to collect data, with an enhanced notice and consent mechanism based on user opt-in, its own apps are notably exempt from this.

Sokol and Zhu (2021) have pointed out the negative competition outcomes likely to result from these policy changes.[21] By weakening third-party apps' ability to target consumers effectively—a positive data protection outcome—Apple will compel many of them to switch from a 'free', ad-supported model to a fee-driven model. Given that all app fees are subject to a 15–30% Apple surcharge, this switch will degrade third-party app developers' revenue stream while enhancing Apple's. It will also lead to de facto self-preferencing of Apple apps that are not subject to a surcharge and can therefore be cheaper than third-party apps, giving Apple a competitive advantage.

This decrease in competition is not merely intra-ecosystem, it is also inter-ecosystem. By compelling third-party apps to switch from an ad-driven to a fee-based revenue model, Apple will also raise costs for consumers switching to the Android platform in two ways. One, if the policy change causes consumers to prefer Apple's apps over third-party rivals, they will find the process of switching to Android—where many of Apple's apps are not available—more cumbersome. Second, even when consumers prefer third-party apps, the fee for a subscription-based model would mean they would have to repurchase the app or lose access to in-app purchases if switching to Android—again creating lock-in.

Google's move to prohibit third-party 'cookies' in its web browser, Chrome, raises similar concerns as the EC's announcement of an antitrust investigation into its online display advertising technology services has noted.[22] Restricting third-party tracking in this manner is not new. Other browsers such as Apple's Safari, Mozilla's Firefox, and Microsoft's Edge have, in fact, done more on this front than Google. This has positive data protection outcomes.

From a competition perspective, however, there is a crucial difference between Chrome's rivals—which cumulatively account for a little under 35% of the global browser market—and Chrome, which has over 65% of the market. By disabling the mechanism that publishers use to target ads and personalize content, Google will potentially entrench its position in the digital advertising business. It is already under investigation for restricting third-party access to user data for advertising purposes, while continuing to use the data in its own ad tech stack. Blocking cookies would leverage this practice, pushing advertisers into its ecosystem that would offer targeting advantages that rivals would not benefit from. Such concentration of advertising spend would further distort competition.

Such attempts to entrench dominance and hamstring competition by using data protection mechanisms are not the only way negative competition outcomes can overlap with positive data protection outcomes. Bigger firms can also actively leverage data protection regulations to their advantage. The GDPR has created multiple opportunities for them to do so. Google has taken advantage of the fact that regulations raise the cost of a firm being in business with its consent tool, Google Funding Choices (GFC). Smaller publishers that lack the capital or capacity to develop their own consent tools in order to comply with GDPR have opted for the convenience of

21 Sokol and Zhu's (2021) broader argument about the consumer welfare benefits of the ad-driven revenue model requires nuance. Given the subjectivity of consumer preferences and information asymmetry, it is not a given that personalized advertising generates net positive consumer surplus. Economides and Lianos (2021) provide an analysis of the importance of consumer choice exercised through markets for data that is particularly relevant.

22 EC press release, 'Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector'(22 July 2021). https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3143; accessed 14 July 2021. The UK's CMA has also launched an investigation, explicitly referring to the contradictory and overlapping data protection and competition imperatives. CMA press release,'CMA to investigate Google's "Privacy Sandbox" browser changes'. https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes; accessed 13 July 2021.

the GFC. While this may very well increase data protection outcomes, it concentrates the digital advertising market further. Publishers must accede to limited choices to be part of the Google ecosystem (Jacobides *et al.*, 2020). Google is thus able to exert pressure on both complementors and other ad-tech companies.

Negative competition outcomes also overlap with better data protection outcomes in a more passive fashion. Given regulatory costs, larger companies with deep pockets have a greater capacity to cover compliance costs than smaller firms These companies are often under more intense scrutiny and are more aware of the reputational risks that bad data practices can raise, including data leakages. The use of regulations as a competition barrier can also be observed in other sectors. For example, in 2013, Amazon lobbied for the introduction of a regulation that would allow US states and local authorities to tax online purchases. This change in legislation arguably benefited Amazon, which was able to ramp up its infrastructure to collect such taxes, while placing a significant burden on its competitors—smaller online retailers around the country.[23]

Some data protection regulations include rules requiring mandatory data sharing, which could lead to less competition and reduce incentives for new firms to enter a market, as revenue generation would be diminished. Also, if data are shared between competitors, commercially relevant information could be used to facilitate collusive practices.

4. Reconciling competition policy and data protection

The previous section described different ways in which competition policy considerations might interact with data protection concerns, highlighting the potential for convergence and divergence between the two. Operationalizing their coexistence effectively will allow regulatory authorities to maximize the benefits of these interactions and reduce the risks of conflicting outcomes.

A two-step analysis is necessary for this. First, what type of relationship should exist between competition law and horizontal sector regulation such as data protection law from a normative perspective? Second, from a positive, practical angle, how can this relationship be translated into procedures that competition authorities and policymakers can implement?

4.1 A normative perspective

An ongoing debate in the current literature is whether an economic policy should consider 'noneconomic' distributional factors. Competition policy results in important social effects—for example, fighting cartels benefits the poorest, while taming abuse of market power contributes to wealth distribution. However, the question about whether competition policy should address fairness and equity remains controversial. Many argue that there are good reasons why distributional issues cannot be ignored, especially from a normative perspective. However, some economists claim that economic policy should be solely about economic efficiency and that using it to redistribute income might lead to distortions in prices and incentives and thus to substantial efficiency losses and unintended effects (Veljanovski, 2010).

Conventional competition law will not be able to address all problems associated with digital platform ecosystems. Some reform proposals overlook the potential to build on normative parameters from data protection regulation and the associated expertise of privacy regulators. Several jurisdictions are now seriously considering the adoption of new regulatory frameworks—in some cases accompanied by the creation of sector-specific regulators—to focus specifically on technology companies operating in digital markets. The most notable proposal aimed at improving competition in these markets is the DMA, announced by the EC in December 2020. The DMA would introduce a differentiated regime for platforms classed as 'gatekeepers', establishing a set of obligations for their behavior—a series of 'dos and don'ts'. In the United Kingdom, a taskforce led by the CMA will design and implement a new pro-competition regime for digital markets to introduce differentiated rules for technology companies that enjoy 'strategic market status'.

23 See Goldstein, J. 'Why Amazon Supports an Online Sales-Tax Bill', NPR, 22 April 2013. https://www.npr.org/sections/money/2013/04/22/178407898/why-amazon-supports-an-online-sales-tax-bill?t=1622811013504; accessed 12 July 2021.

Animating these proposals is the argument that competition law alone will not be able to fix the flaws of digital markets and that there is a need for a more detailed *ex ante* prescriptive regulatory intervention. Some academics argue that, rather than pushing for an entirely new set of regulations, authorities should seriously consider the potential of existing data protection rules to address emerging problems (Monti, 2020). From a normative angle, the question is whether competition authorities should consider privacy and data protection issues in some of their decision-making processes. A normative investigation into the role of data protection in competition policy would therefore depend on the foundations of the policy, that is, its goals and scope.

4.1.1 The goals and scope of competition law

The digital markets addressed in this article do not comply with traditional price structures, and market power of digital platform ecosystems can no longer be assessed solely in terms of monetary prices. The traditional drivers of competition, such as price efficiency and low cost, are now being replaced by data-related innovation and differentiation by platforms and ecosystems (Jenny, 2021). However, there is an increasing focus on how competition policy itself needs to be revamped to meet the challenges of digital platforms. Biggar and Heimler (2021) specifically address the question of how competition law is inadequate in its current scope to curtail digital platforms' anticompetitive practices and needs to move away from the consumer welfare standard toward a transaction costs framework that accounts for the dependency generated by ecosystems that lock in both their consumers and their suppliers.

This is particularly relevant when competition authorities have a broader public interest mandate from governments. For example, in South Africa, the purposes of competition law also include 'advancing the social and economic welfare of South Africans, and ensuring that small- and medium-sized enterprises have an equitable opportunity to participate in the economy' (Koornhof and Pistorius, 2018). In such jurisdictions, there is a clear possibility of broadening the scope of regulatory goals to incorporate data protection concerns and principles.

In jurisdictions with consumer-welfare-centric competition frameworks, the characteristics of the data-driven economy make it necessary to include privacy considerations in competition assessment. As argued, the defense of the consumer welfare standard is one of the cornerstones of competition law in most jurisdictions.[24] In contrast, data protection legislation is more akin to consumer protection law in that it is aimed at protecting individual users' rights (Ohlhausen and Okuliar, 2015). As we explored in Section 3, there are considerable overlaps between the two regulatory regimes. Data protection determines the legitimate limits for the collection and processing of data that inform competitive parameters such as price and quality. Crucially, it also lays down the optimal level of control users should have over their data, which allows them to reveal their preferences regarding privacy and data protection more accurately. Both therefore guard against the exploitative use of market power (Costa-Cabral and Lynskey, 2017). A key difference is that competition law imposes specific duties on firms that hold power in a given market, while data protection regulation usually applies horizontally to all companies engaged in data collection and processing, regardless of their size. This means that while the asymmetry between user and company is a relevant aspect in the competition analysis, it might not be relevant for the enforcement of data protection law.

Their relationship can be operationalized either by broadening the scope of competition law to pursue goals related to data protection or by incorporating data protection concerns as a dimension of consumer protection. An effective approach must address the importance of institutional coordination between different regulatory bodies in these areas, given the need for complementary expertise. Graef *et al.* (2018) explore the relationship between competition, data protection, and consumer law, arguing that there are concrete instances where those areas 'can be applied more coherently and where the relevant authorities can collaborate more closely in order to achieve a better protection of consumer interests'. An interesting example of this type

24 As emphasized by Ezrachi (2017), although the concept of 'consumer welfare' is often referred to as a leading universal benchmark, it does not embody universally agreed properties, and jurisdictions often diverge as to the exact meaning of the term and how to achieve it.

of collaboration is the case against Facebook, investigated by the German competition regulator, the Bundeskartellamt, while the Italian counterpart sanctioned Facebook for a similar behavior under consumer law rather than competition law (Botta and Wiedemann, 2019). This points to scenarios in the future where regulation of digital platforms will require coordination under different laws and thus authorities. The European Data Protection Supervisor's notion of a 'digital clearing house' for regulatory coordination is an explicit recognition of these overlaps.

Another example is the creation of a dedicated digital markets taskforce by the UK Government, which gathers representatives from the CMA, the Office of Communications, and the Information Commissioner's Office. There is precedent for such coordination and for a polycentric approach where other regulatory rules or legislation inform competition regulation. India's Competition Act 2002, for instance, provides a series of exceptions for terms and conditions that protect intellectual property rights, regardless of other provisions in the Act.[25] Across jurisdictions, intellectual property law has also given competition regulators normative guidance for assessing innovation as a competitive parameter. More broadly, the European Court of Justice ruled in 2013 in the Allianz Hungária case (a vertical agreement between the insurers and motor repairers in Hungary) that competition regulation could take the objectives of other national rules on board in its assessment.[26] Therefore, there are reasons in various jurisdictions for data protection rules to provide normative guidance to competition regulation in assessing exploitative conduct on digital platforms.

4.2 A positive perspective

From a positive perspective, the key issue is how to incorporate privacy considerations into competition authorities' analysis to help them deliver their goals, regardless of the specific competition policy aims. At the policy level, integrating privacy considerations into competition regulation can be considered a requirement of the digital age. Competition authorities around the world can differ in the nature of their mandate, but a positive perspective can be useful to inform policymakers about the different ways competitive outcomes interact with privacy outcomes. A positive perspective would be pertinent, given that literature on the ways that competition on digital platforms and ecosystems differs from traditional platforms is expanding (Jenny, 2021). Some of these interactions are explored below.

4.2.1 Analytical steps

Privacy and data protection can be incorporated as relevant parameters to inform two key analytical steps of any antitrust case: the definition of the relevant market and the assessment of market power. Existing theory and evidence suggest that firms' access to personal data influences the propensity to enter markets and the outcomes experienced within markets. This makes data collection and processing relevant for competition authorities (see Section 2.1). Thus, recognizing the differences in privacy preferences might help policymakers design policies that are more effective in inducing compliance with competition law. For example, it might affect the incentives for firms to access users' data.

Some scholars argue that, for digital platforms which offer services at 'zero' price in exchange for personal data, the assessment of market power should account for a company's ability to reduce the level of data protection (Esayas, 2018a). The challenge remains, however, which proxy to use to address the privacy considerations behind the collection and use of personal data to assess market power. For example, alternative metrics of market power in zero-price digital platforms can include the total number of users, active users, or time spent on a given service (Evans, 2013; Esayas, 2018a; Wu, 2019).

Conversely, market structure and the level of dominance of a given firm can play a role in the enforcement of data protection rules. Due to the relevance of data to identify markets and assess market power, some scholars have argued that these concepts should be used to help interpret the

25 Section 3(5) of India's Competition Act, 2002, carves out wide-ranging exceptions under the Copyright Act, 1957, Patents Act, 1970, Trade Marks Act, 1999, Geographical Indications of Goods (Registration and Protection) Act, 1999, Design Act, 2000, and Semiconductor Integrated Circuits Layout-Design Act, 2000.

26 See the European Union Court of Justice (ECJ), 'Allianz Hungária', Case C-32/11, judgment of 14 March 2013.

compliance obligations that data controllers and data processors have under data protection law. Such a proposal would be compatible, for example, with the risk-based approach of the GDPR (Graef *et al.*, 2018).

4.2.2 Merger control

Data considerations are essential to inform merger control in digital markets. Since 1986, there have been 825 mergers and acquisitions (M&A) by the major digital companies, namely Google, Apple and Facebook. M&A activity has seen a significant rise over the past few years (Parker *et al.*, 2021). Increased data concentration through M&A exacerbates the net negative overlap of competition and data protection outcomes that we outlined earlier (see Section 3.1). For instance, consumer protection organizations have been pressuring competition authorities around the world to investigate Google's acquisition of Fitbit (a company that produces a smartwatch that digitally tracks health activity) due to data concentration concerns. They argue that the processing of personal data by the merged company can be used to deteriorate the quality of services and, consequently, competition in both the digital and health-care markets.[27]

While acknowledging 'privacy' as a component of product quality and as a parameter of non-price competition, competition authorities are yet to veto a merger between companies on the basis of such concerns.[28] An analysis of case law suggests that privacy-related concerns due to data concentration were not within the bailiwick of competition regulation. This apparently contradictory interpretation stems from the dominant monocentric approach that assesses consumer preferences using a monetary price-centric model (Lianos, 2019). This model cannot account for the distortionary effect of zero-price on consumer preferences or data costs and information asymmetry and therefore chooses simply to ignore them. Importantly, the assessment conducted by competition authorities to date tends to assume that privacy concerns will be addressed by the relevant data protection authority, which would allegedly be best placed to conduct investigations.

A merger assessment that aims at regulatory convergence between competition and data protection frameworks is essential for rectifying this. The EC took the first step in the Facebook–WhatsApp and Microsoft–LinkedIn mergers. In these cases, the EC called for privacy to be used as a parameter in merger assessment, when privacy was an important area of competition between the entities, or if data concentration would harm competition on privacy (Giannino, 2017). However, the implementation of such assessment was flawed, as it did not prevent Facebook from acquiring WhatsApp and subsequently combining data from both platforms. While the US Federal Trade Commission brought a case against Facebook, alleging that its acquisitions of WhatsApp and Instagram were anticompetitive, this was not on the grounds of privacy.[29] The European Data Protection Board also warned that Google's acquisition of Fitbit could have long-term privacy implications and called for a transparent data protection assessment.[30] However, any such assessment is likely to run into similar methodological issues.[31]

Drawing on data protection frameworks to develop methodologies for assessing mergers from the perspective of data concentration and privacy would give competition regulators clearer parameters. For example, India's draft Data Protection Bill, 2019, envisions a Data Protection Authority that will publish 'Codes of Practice'. Such secondary legislation would establish standards and guidelines for data protection issues such as anonymization, PETs, and

27 See Common Statement by Consumer and Citizen Groups on Google Fitbit Takeover, 2 July 2020, https://www.beuc.eu/publications/consumer-and-citizen-groups-have-serious-concerns-about-google-fitbit-takeover; accessed 12 July 2021.

28 Data concentration issues were first highlighted by antitrust authorities in the Google-DoubleClick merger in 2008 (Kimmel and Kestenbaum 2014); Google and Facebook have acquired 168 and 71 companies, respectively, in the subsequent decade until 2018 (Argentesi *et al.*, 2021).

29 The case was recently dismissed by the Federal Court as the Federal Commission failed to prove Facebook was a monopoly.

30 See European Data Protection Board Statement on Privacy Implications of Mergers, adopted on 19 February 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf; accessed 12 July 2021.

31 For example, the EC has a peculiar logic of privacy substitutability: it held that the differing levels of privacy offered by Facebook and WhatsApp pre-merger showed that they were complementary services rather than competitors, instead of recognizing that the degree of privacy is a vector of competition (Esayas, 2018b).

data minimization. Competition authorities can draw on similar frameworks to enrich their understanding of multi-dimensional competition on privacy and guide their assessments.

The existing framework to assess M&A for most digital platforms will need to take into account more dynamic factors of data-related synergies. It should also broaden the field of competition to assess various complementary markets and ecosystems and balance the efficiency gains against the anticompetitive concerns (Parker *et al.*, 2021). Given that these online platforms are typically multisided, the review of mergers must take into account the impact on either side of the markets. In the case of ecosystems, the actions of the dominant player must be scrutinized to assess the impact of acquisitions on the downstream and upstream market as well (Jacobides and Lianos, 2021; Parker *et al.*, 2021). Competition authorities may also resort to novel merger remedies based on data protection considerations, such as requiring merging parties to keep their databases separate or create a firewall between them (Graef *et al.*, 2018). However, the inclusion of specific conditions to protect privacy in settlement agreements or consent decrees as part of a merger approval would only be effective if there were enforcement mechanisms This would be akin to a *quasi*-regulatory intervention, which creates the need for constant monitoring to ensure compliance and to make sure the remedies remain effective and proportional over time. More specifically, it would require monitoring the resulting merged enterprise to ensure that data are not shared between the previously distinct services. This would be more effective with a robust data protection framework (Kimmelman *et al.*, 2018). One trend observed in other jurisdictions—for example, the Australian Competition and Consumer Commission (ACCC) and the UK's CMA—is the establishment of digital or data science units, which would be more prepared to ensure compliance with remedies and detect and obtain evidence of competition issues in digital markets (World Bank, 2021).

Data considerations are relevant to the *ex ante* review of concentrations but could inform the design of structural remedies to restore the competitive process in the market. The adoption of behavioral remedies such as strengthened access requirements, nondiscrimination provisions, and interoperability may not always be sufficient to address structural flaws. To dislodge entrenched dominance and to fundamentally alter the concentrated market structure that gives rise to anticompetitive behavior, more radical interventions such as mandatory divestiture or reversing consolidated mergers—measures often labeled as 'breakups'—may be necessary (Kwoka and Valletti, 2021). In these circumstances, understanding the role played by different types of data in the architecture of firms can help to identify what Kwoka and Valletti (2021) call the 'natural break points' in merged firms that could lead to a more successful restructuring of their businesses. For example, breakups force the structural separation of data sets, thus preventing the misuse of data on rivals and their customers, and making it more difficult for companies to draw unwanted inferences about their users.

4.2.3 Anticompetitive behavior

Data protection considerations can also provide objective parameters to assess consumer welfare losses related to subjective data costs, which can be associated with anticompetitive behavior. While monetary costs are fungible and therefore provide a direct way to quantify such trade-offs in conventional markets, data costs are subjective and qualitative. Consumers may surrender differentiated data for the same product; many data fields are optional while signing up on digital platforms The nature, length, and frequency of advertisements they will be targeted with based on their data will also be different, as will their appetite for privacy and control over their data (Newman, 2015).

Quality effects are similarly subjective. Consumer preferences on digital platforms—particularly in zero-price markets—are complex. The positive and negative quality effects of reduced privacy have the same origin and may offset each other. There is no clear way to quantify subjective consumer experience and preference: some consumers may not experience the negative effects of concealed data practices and may therefore experience the loss of privacy in exchange for a zero-price product as an increase in quality.

Some commentators are skeptical of seeing 'competition on privacy' with its associated consumer welfare as a competition regulation problem (Manne and Sperry, 2015). This argument rests on two false assumptions. The first is that the 'notice and choice' model prevalent in the

digital economy enables consumers to make a rational choice based on a meaningful ability to assess transaction costs and manage privacy boundaries. This is undermined by the reality of concealed data practices: the notice is incomplete, misleading, deliberately vague, and often subject to unilateral change by companies (Kemp, 2020). For instance, research shows that users believe that privacy policies stop companies from sharing their data with anyone or using it in ways that they would consider misuse—both demonstrably false (ACCC, 2019; Consumer Policy Research Centre, 2019).

The second assumption is that the subjectivity of data costs renders the consumer-facing market of digital platforms immune to antitrust regulation. While monetary costs are objective, antitrust assessment can be subjective in conventional markets as well. Revealed consumer preferences are, in some ways, taken on faith as much as calculation, given the distortionary effects of information asymmetry. The barrier therefore is not subjectivity. In conventional markets, competition law has constructed a normative framework to assess distortionary practices. Data protection regulation can provide the much-needed parameter for zero-price digital platforms.

As noted earlier, data protection can provide a normative framework that delineates legally acceptable methods of data collection and processing. Creating a new framework for competition assessment of digital platforms would be 'reinventing the wheel'. It would also potentially create divergent understandings of key regulatory elements that straddle the two regimes. The Bundeskartellamt's ruling against Facebook that Germany's Federal Court of Justice has now put back on track is the 'canary in the coalmine'. Andreas Mundt, president of the German competition authority, explicitly noted at the time of the preliminary findings that '[d]ata protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company'.[32]

The ruling expands on this logic, finding that Facebook's terms violated the GDPR by making use of the platform in Germany conditional on gathering and combining user and device data from other services without obtaining effective consent—the company was therefore guilty of abusive practice under competition law. The Bundeskartellamt report said:

> [..] the stipulated control of data processing policies cannot mean that, in its task of monitoring the scope of data processing, the competition authority should disregard the principles of general data protection law and develop its own benchmark or other tools instead [..] As shown by the case-law on VBL-Gegenwert, an abuse of a dominant position can be caused by the fact that a company did not even comply with the general legal framework. The control of abusive practices with respect to the scope for data processing must therefore also include compliance with data protection law.[33]

This lays out a clear path for using data protection legislation to inform competition assessment when identifying exploitative conduct by dominant platforms that impinges on consumer welfare. This logic can also be extended to data costs and the quality of product. For example, a unilateral decrease in user control over personal data or an increase in data sharing and processing at the supplier backend that violate the terms of data protection legislation could similarly be considered exploitative (Costa-Cabral and Lynskey, 2017). This approach could also fit within a more conventional Rule of Reason analysis. In *Ohio v. American Express Co*, the US Supreme Court ruled that the first stage of the burden-shifting framework used in such analysis consisted of showing evidence of detrimental effects on competition via 'reduced output, increased prices or decreased quality in the relevant market'.[34] Leaving aside the fact that defining a relevant market is not necessary at this stage (Hovenkamp, 2019), understanding that data are a nonmonetary cost and loss of privacy and control of personal data are a metric of decreased quality—both

32 See the Bundeskartellamt statement on Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources are abusive, 19 December 2017, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html.

33 See decision under Section 32(1) German Competition Act (GWB) by Bundeskartellamt, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5; accessed 14 July 2021.

34 See Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018). https://lexroll.com/ohio-v-american-express-co-138-s-ct-2274-2018; accessed 14 July 2021.

benchmarked against data protection regulation for legitimacy—could allow regulators to assess anticompetitive effects within a Rule of Reason evidentiary framework. This will be challenging to implement, particularly when few antitrust cases emerge from the burden-shifting process as true positives. However, we feel that it merits further study.

5. Conclusion

This article argues that multiple interfaces between competition policy and data protection should be considered in the analysis of digital markets. Drawing from case law and market studies from different countries, we identify the issues arising from the substantive overlap between the two regimes and discuss the contours of a more holistic framing to integrate privacy and data protection considerations into competition policy. There are many cases where data protection and competition considerations align, leading to similar outcomes (either positive or negative). In these situations, adopting an integrated regulatory approach can foster positive synergies between the two sets of rules. However, there are also situations where their concomitant application can lead to contrasting outcomes. Even though these situations are less common, an integrated approach is even more important to reduce the risk of conflicting policy outcomes.

Because this article is not restricted to the legal regime of any particular jurisdiction, we do not offer a fully fledged and all-encompassing reform proposal to address the issue we identify. There are significant international differences in approaches to data protection and competition policy, and competition authorities around the world differ in their mandate and in the scope of their competition laws. Data privacy and data protection also vary across countries and are often dependent on underlying cultural norms, which evolve over time. However, there are general steps that can be taken by policymakers and practitioners working in different contexts where competition policy and data protection regimes interact:

- From a normative angle, we argue that data protection considerations should inform competition authorities' and regulators' assessment of digital platforms and decision-making processes, in jurisdictions that adopt a wider scope for competition law, and those that follow a more conventional consumer protection standard of enforcement. This includes the consideration of the role of data for the establishment of competitive parameters such as nonmonetary price, innovation, and quality and also as a benchmark for the assessment of exploitative conduct.
- From a positive perspective, we suggest practical ways to integrate privacy considerations into competition regulation. We argue that assessing the implications of competition policy for data protection may offer an opportunity for competition authorities to contribute to the protection of the fundamental right to privacy, without necessarily changing the focus on consumer welfare. Data protection could also help to address market failures emerging from digital platforms' business models.

Ultimately, the holistic approach we propose requires a broader approach beyond digital markets. It means reconsidering the relationship between the two instruments of market supervision and framing them as adjacent and overlapping sections of the same regulatory continuum. While the debate on the effective supervision of markets is often framed around whether competition law or sectoral regulation would be the most appropriate tool to address the challenges of digitalization, in practice, the boundary between these two instruments is often not as clearly defined as the literature seems to imply.

The regulatory instrument that emerges from the interaction between competition law and economic regulation has been called 'regulatory competition law', or 'competition law-as-regulation' (Dunne, 2015). These terms are used to describe situations where competition law deviates from its traditional 'core' conception and assumes features more commonly associated

with economic regulation, that is, situations where competition law assumes some of the characteristics commonly associated with sectoral or horizontal regulation.

In practice, this requires competition policy actors and institutions to establish an understanding of data protection and privacy regulation and develop expertise across policy boundaries. Some scholars argue that this would entail competition authorities and information regulators or data protection authorities entering into formal cooperation agreements. This arrangement, alongside addressing potential anticompetitive data use, would also avoid unnecessary additional regulation for data processors (Koornhof and Pistorius, 2018). The Brazilian competition authority, for example, recently lobbied to absorb the competences of the national data protection authority. The country is debating how to create a new regulator in the context of severe budgetary constraints—a proposal that has not been taken forward by the government. Other practical measures include amending the relevant legislation and guidelines to expressly allow authorities to consider data protection when enforcing competition law.

Addressing all concerns emerging from the data economy will require an integrated approach from many other regulatory perspectives. Even though competition policy has a relevant role to play in protecting data, and vice versa, neither framework should be considered a replacement for the other, nor as a ubiquitous tool to redress the potential harms in digital markets. Finally, the nature of competition in platform-based ecosystems provokes a wider discussion and points to an important research agenda about the suitability of competition law tools and its underpinning theory to deal with the challenges of contemporary capitalism.

Acknowledgments

The authors would like to thank Michael Jacobides, Anupam Manur, two anonymous reviewers, and the editors of this journal for their helpful comments and suggestions on earlier drafts of this article. The article greatly benefitted from discussions with Geeta Gouri, Hemangini Dadwal, Puneeth Nagaraj, Stefan Dercon, Benno Ndulu, Elizabeth Stuart, Toby Phillips, Matthew Sharp, as well as the participants at the Blavatnik School of Government research seminar and the Data Governance Network roundtable discussion. We are also thankful to Beth Keehn for copyediting. All errors and omissions remain our own.

Funding

Research funded by Global Challenges Research Fund and Omidyar Network.

References

Argentesi, E., P. Buccirossi, E. Calvano, T. Duso, A. Marrazzo and S. Nava (2021), 'Merger policy in digital markets: an ex post assessment,' *Journal of Competition Law & Economics*, **17**(1), 95–140.

Australian Competition and Consumer Commission (2019), 'Digital Platforms Enquiry,' https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/final-report-executive-summary.

Barnes, S. B. (2006), 'A privacy paradox: social networking in the United States,' *First Monday*, **11**(9), 1–3.

Biggar, D. and A. Heimler (2021), 'Digital platforms and the transactions cost approach to competition law,' Working Paper (Under Review, ICC).

Borghi, M. (2019), *Data Portability and Regulation of Digital Markets*. Centre for Intellectual Property Policy and Management. Bournemouth University: UK.

Botta, M. and K. Wiedemann (2019), 'The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook Odyssey,' *The Antitrust Bulletin*, **64**(3), 428–446.

Bradford, A. (2020), *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Brynjolfsson, E. and A. Collis (2019), 'How should we measure the digital economy,' *Harvard Business Review*, **97**(6), 140–148.

Brynjolfsson, E., F. Eggers and A. Collis (2019), 'Using massive online choice experiments to measure changes in well-being,' *Proceedings of the National Academy of Sciences*, **116**(15), 201815663.

Bundeskartellamt (2016), 'Competition Law and Data,' https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=50588C5CDD10808F9DEDE8B5B2654CA5.2_cid387?__blob=publicationFile&v=2.
Caffarra, C., F. Etto, O. Latham and F. Scott Morton (2020), 'Designing regulation for digital platforms: why economists need to work on business models,' *EUVox*. https://voxeu.org/article/designing-regulation-digital-platforms.
Casadesus-Masanell, R. and A. Hervas-Drane (2015), 'Competing with privacy,' *Management Science*, **61**(1), 229–246.
Competition Law Review Committee (2019), 'Report of the competition law review committee,' Ministry of Corporate Affairs, Government of India. http://www.mca.gov.in/Ministry/pdf/ReportCLRC_14082019.pdf.
Condorelli, D. and J. Padilla (2020), 'Data-driven envelopment with privacy-policy tying.' https://ssrn.com/abstract=3600725.
Consumer Policy Research Centre (2019), 'Submission to the consultation on the ACCC digital platforms inquiry preliminary report December 2018.' Consumer Policy Research Centre: Melbourne.
Costa-Cabral, F. and O. Lynskey (2017), 'Family ties: the intersection between data protection and competition in EU law,' *Common Market Law Review*, **54**(1), 11–50.
Cowen, T. (2018), 'Why forced data portability is a mistake,' *Marginal Revolution*. https://marginalrevolution.com/marginalrevolution/2018/05/forced-data-portability-mistake.html.
Crémer, J., Y. A. de Montjoye and H. Schweitzer (2019), *Competition Policy for the Digital Era*. European Commission. Publications Office of the European Union: Luxembourg.
Cusumano, M. A., A. Gawer and D. B. Yoffie (2021), 'Can self-regulation save digital platforms?' *Working Paper (Under Review, ICC)*.
DeLong, J. B. and A. M. Froomkin (2000), 'Speculative microeconomics for tomorrow's economy,' in B. Kahin and H. R. Varian (eds.), *Internet publishing and beyond: The economics of digital information and intellectual property*. The MIT Press: Cambridge, MA, pp. 6–44.
Dunne, N. (2015), *Competition Law and Economic Regulation: Making and Managing Markets*. Cambridge: Cambridge University Press.
Economides, N. and I. Lianos (2021), 'Restrictions on privacy and exploitation in the digital economy: a market failure perspective,' *NET Institute Working Paper No. #20-05*, NYU Stern School of Business.
EDPS (2014), 'Privacy and Competitiveness in the Age of Big Data: the interplay between data protection, competition law and consumer protection in the digital economy.' European Data Protection Supervisor: Brussels. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.
Eisenmann, T., P. Geoffrey and M. Van Alstyne (2011), 'Platform envelopment,' *Strategic Management Journal*, **32**(12), 1270–1285.
Esayas, S. Y. (2018a), 'Competition in (Data) Privacy: 'Zero'-price markets, market power, and the role of competition law,' *International Data Privacy Law*, **8**(3), 181–199.
Esayas, S. Y. (2018b), 'Data privacy in European merger control: critical analysis of commission decisions regarding privacy as a non-price competition,' *European Competition Law Review*, **40**(4), 166–181.
Evans, D. S. (2003), 'The antitrust economics of two-sided markets,' *Yale Journal on Regulation*, **20**(2), 325–381.
Evans, D. S. (2011), 'Antitrust economics of free,' *Competition Policy International*, **7**. https://www.competitionpolicyinternational.com/the-antitrust-economics-of-free/.
Evans, D. S. (2013), 'Attention rivalry among online platforms,' *Journal of Competition Law & Economics*, **9**(2), 313–357.
Evans, D. S. and R. Schmalensee (2016), *Matchmakers: The New Economics of Multisided Platforms*. Harvard Business Review Press: Boston.
Ezrachi, A. (2017), 'Sponge,' *Journal of Antitrust Enforcement*, **5**(1), 49–75.
Ezrachi, A. and M. E.Stucke, (2015), 'The curious case of competition and quality,' *Journal of Antitrust Enforcement*, **3**(2), 227–257.
Furman, J., D. Coyle, A. Fletcher, P. Marsden and D. McAuley (2019), 'Unlocking digital competition,' Report of the Digital Competition Expert Panel. HM Treasury: London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.
Gal, M. and O. Aviv (2020), 'The unintended competitive consequences of the GDPR,' *Journal of Competition Law and Economics*, **16**(3), 349–391.
Galbraith, J. K. (1995), 'The winner takes all… sometimes,' *Harvard Business Review*, **73**(6), 44–45.
Geradin, D. (2021), 'What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a digital market act?' Tilburg Law and Economics Center (TILEC); Geradin Partners; University of East Anglia (UEA) - Centre for Competition Policy; University College London - Faculty of Laws.10.2139/ssrn.3788152.

Giannino, M. (2017), Microsoft/LinkedIn: what the European Commission said on the competition review of digital market mergers.
Goldstein, J. (2013), 'Why Amazon Supports an Online Sales-Tax Bill,' NPR, 22 April. https://www.npr.org/sections/money/2013/04/22/178407898/why-amazon-supports-an-online-sales-tax-bill?t=1622811013504.
González Fuster, G. (2014), 'The emergence of personal data protection as a fundamental right of the EU,' Law, Governance and Technology Series, vol 16. New York: Springer.
Graef, I., D. Clifford and P. Valcke (2018), 'Fairness and enforcement: bridging competition, data protection, and consumer law,' *International Data Privacy Law*, **8**(3), 200–223.
Graef, I., T. Tombal and A. De Streel (2019), 'Limits and enablers of data sharing. An analytical framework for EU competition, data protection and consumer law,' *TILEC Discussion Paper No. DP 2019–024*. Tilburg Law and Economics Center (TILEC): The Netherlands.
Greenleaf, G. (2021), 'Global data privacy laws 2021: despite COVID Delays, 145 laws show GDPR dominance,' 169 Privacy Laws & Business International Report, 1, 3–5, UNSW Law Research.
Hoofnagle, C. J. and J. Whittington (2014), 'Free: accounting for the costs of the internet's most popular price,' *UCLA Law Review* 61. https://www.uclalawreview.org/pdf/61-3-2.pdf.
Hovenkamp, H. (2020), 'Antitrust's borderline,' *University of Pennsylvania, Institute for Law & Economic Research Paper No. 20–44*. University of Pennsylvania Institute for Law & Economics: Philadelphia.
Hovenkamp, H. J. (2019), 'Platforms and the rule of reason: the American Express case,' *Columbia Business Law Review*, **35**(1), 34–92.
Ibáñez Colomo, P. (2016), 'Beyond the 'More Economics-based Approach': a legal perspective on Article 102 TFEU case law,' *Common Market Law Review*, **53**(3), 709–739. http://eprints.lse.ac.uk/id/eprint/65776.
Jacobides, M., M. Bruncko and R. Langen (2020), 'Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference,' London Business School: London. https://ssrn.com/abstract=3765324.
Jacobides, M., T. Knudsen and M. Augier (2006), 'Benefiting from innovation: value creation, value appropriation and the role of industry architectures,' *Research Policy*, **35**(8), 1200–1221.
Jacobides, M. and I. Lianos (2021), 'Ecosystems and competition law in theory and practice,' Centre for Law, Economics and Society Research Paper Series 1/2021. University College London: London. https://www.ucl.ac.uk/cles/sites/cles/files/cles-1-2021.pdf.
Jacobides, M., A. Sundararajan and M. Van Alstyne (2019), 'Platforms and ecosystems: enabling the digital economy,' World Economic Forum Briefing Paper. World Economic Forum: Switzerland.
Jatania, B. (2019), *Antitrust and Zero-price Digital Platforms: An Indian Regulatory Approach*. IDFC Institute: Mumbai. http://www.idfcinstitute.org/site/assets/files/15463/idfc_bhusan_antitrust_-_paper_1.pdf.
Jenny, F. (2021), 'Competition law enforcement and regulation for digital platforms and ecosystems: understanding the issues, facing the challenges and moving forward,' *Working Paper (Under Review, ICC)*.
Kemp, K. (2020), 'Concealed data practices and competition law: why privacy matters,' *European Competition Journal*, **16**(2–3), 628–672.
Kerber, W. (2016), 'Digital markets, data, and privacy: competition law, consumer law and data protection,' *Journal of Intellectual Property Law & Practice*, **11**(11), 856–866.
Khan, L. M. (2017), 'Amazon's antitrust paradox,' *Yale Law Journal*, **126**(3), 710–805.
Khan, L. M. (2019), 'The separation of platforms and commerce,' *Columbia Law Review*, **119**(4), 973–1098.
Kimmel, L. and J. Kestenbaum (2014), 'What's up with whatsapp? A transatlantic view on privacy and merger enforcement in digital markets,' *Antitrust*, **29**(1). http://awa2015.concurrences.com/IMG/pdf/fall14-kimmel_c_.pdf.
Kimmelman, E., H. Feld and A. Rossi (2018), 'The limits of antitrust in privacy protection,' *International Data Privacy Law*, **8**(3), 270–276.
Koornhof, P. and T. Pistorius (2018), 'Convergence between competition and data protection law: a South African perspective,' *International Data Privacy Law*, **8**(3), 277–283.
Kwoka, J. and T. Valletti (2021), 'Unscrambling the eggs: Breaking up consummated mergers and dominant firms,' *Working Paper (Under Review, ICC)*.
Lancieri, F. M. and P. Sakowski (2020), 'Competition in digital markets: a review of expert reports,' *Stigler Center Working Paper Series No. 303*, Stanford Journal of Law, Business & Finance. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681322.
Lianos, I. (2018), 'Polycentric competition law,' Centre for Law, Economics and Society. CLES Research Paper Series No 4. University College London: London. https://www.ucl.ac.uk/cles/sites/cles/files/cles_4-2018_final.pdf.
Lianos, I. (2019), 'Competition law for a complex economy,' *IIC*, **50**, 643–648.
Lianos, I. and A. Ivanov eds (2019), *Digital Era Competition: A BRICS View*. BRICS Competition Law and Policy Centre: Moscow.

Lynskey, O. (2018), 'At the crossroads of data protection and competition law: time to take stock,' *International Data Privacy Law*, **8**(3), 179–180.
Malgieri, G. and B. Custers (2018), 'Pricing privacy – the right to know the value of your personal data,' *Computer Law & Security Review*, **34**(2), 289–303.
Manne, G. and R. Sperry (2015), 'The problems and perils of bootstrapping privacy and data into an antitrust framework,' *CPI Antitrust Chronicle*. https://ssrn.com/abstract=2617685.
Martens, B. (2016), *An Economic Policy Perspective on Online Platforms*. Joint Research Centre: Spain. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2783656.
Mayer, J. (2018), 'Government hacking,' *Yale Law Journal*, **127**(570).
MeitY (2020), 'Report by the Committee of Experts on Non-Personal Data Governance Framework,' Ministry of Electronics and Information Technology, Government of India: New Delhi. https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.
Monti, G. (2020), 'Attention intermediaries: regulatory options and their institutional implications,' *TILEC Discussion Paper, DP 2020–018*. Tilburg Law and Economics Center (TILEC): The Netherlands. http://ssrn.com/abstract=3646264.
Morton, F. and D. Dinielli (2020), *Roadmap for a Monopolization Case against Google Regarding the Search Market*. Omidyar Network. https://omidyar.com/contact/.
Newman, J. (2015), 'Antitrust in zero-price markets: applications,' *Washington University Law Review*, Vol. 94, No. 1, 2016. University of Memphis Legal Studies Research Paper No. 150.
OECD Secretariat (2018), Considering non-price effects in merger control [Background for Item 4 at the 129th Meeting of the Competition Committee on 6–8 June 2018]. Organisation for Economic Co-operation and Development: Paris. https://one.oecd.org/document/DAF/COMP(2018)2/en/pdf.
Ohlhausen, M. K. and A. Okuliar (2015), 'Competition, consumer protection, and the right (approach) to privacy,' *Antitrust Law Journal*, **80**(1), 121–156.
Parker, G., G. Petropoulos and M. Van Alstyne (2021), 'Platform mergers and antitrust,' *Working Paper (Under Review, ICC)*.
Preibusch, S. and J. Bonneau (2013), 'The privacy landscape: product differentiation on data collection,' in B. Schneier (ed), *Economics of Information Security and Privacy III*. Springer: New York, pp. 263–283.
Reyna, A. (2018), 'The psychology of privacy—what can behavioural economics contribute to competition in digital markets?' *International Data Privacy Law*, **8**(3), 240–252.
Robertson, V. (2020), 'Excessive data collection: privacy considerations and abuse of dominance in the era of big data,' *Common Market Law Review*, **57**(1), 161–190.
Scott Morton, F. *et al.* (2019), *Committee for the Study of Digital Platforms: Market Structure and Antitrust Subcommittee Report*. Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business: Chicago.
Shapiro, C. (2019), 'Protecting competition in the American economy: merger control, tech titans, labor markets,' *Journal of Economic Perspectives*, **33**(3), 69–93.
Sokol, D. and F. Zhu (2021), 'Harming competition and consumers under the guise of protecting privacy: an analysis of Apple's iOS 14 policy updates,' USC Law Legal Studies Paper No. 21–27.
Solove, D. J. (2012), 'Introduction: privacy self-management and the consent dilemma,' *Harvard Law Review*, **126**, 1880.
Solove, D. J. (2021), 'The myth of the privacy paradox,' GWU Legal Studies Research Paper No. 2020–10, GWU Law School Public Law Research Paper No. 2020–10.
Solove, D. J. and W. Hartzog (2014), 'The FTC and the new common law of privacy,' *Columbia Law Review*, **114**(3), 583–676.
Stucke, M. E. (2012), 'Behavioral antitrust and monopolization,' *Journal of Competition Law & Economics*, **8**, 545–574.
Stucke, M. E. (2018), 'Should we be concerned about data-opolies?' *Georgetown Law Technology Review*, **275**(2), 275–324.
Stucke, M. E. and A. P. Grunes (2016), *Big Data and Competition Policy*. Oxford: Oxford University Press.
Tisné, M. (2020), *The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective*. Stanford Cyber Policy Center. Stanford University: Stanford CA. https://cyber.fsi.stanford.edu/publication/data-delusion.
Tombal, T. (2021), 'GDPR as shield to a data sharing remedy,' *Deep diving into data protection: 1979–2019: celebrating 40 years of research on privacy data protection at the CRIDS* (Collection du CRIDS; No. 51). Larcier: Brussels, pp. 67–93.
Turck, M. (2016), 'The power of data network effects,' http://mattturck.com/2016/01/04/the-power-of-data-network-effects.

US House Judiciary Committee (2020), Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations. Subcommittee on Antitrust, Commercial, and Administrative Law Committee on the Judiciary, US House of Representatives: Washington.
Varian, H., J. Farrell and C. Shapiro (2004), *The Economics of Information Technology*. Cambridge University Press: Cambridge. https://EconPapers.repec.org/RePEc:cup:cbooks:9780521605212.
Véliz, C. (2020), *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. London: Penguin Books.
Veljanovski, C. (2010), 'Economic approaches to regulation,' in R. Baldwin, M. Cave, and M. Lodge (eds.), *The Oxford Handbook of Regulation*. Oxford University Press: Oxford, pp. 17–38.
Wachter, S. and B. D. Mittelstadt (2019), 'A right to reasonable inferences: re-thinking data protection law in the age of big data and AI,' *Columbia Business Law Review*, **2**, 443–493.
Waehrer, K. (2016), *Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions*. Bates White Economic Consulting: Washington.
Warren, S. D. and L. D. Brandeis (1890), 'The right to privacy,' *Harvard Law Review*, **4**(5), 193–220.
Wils, W. P. J. (2014), 'The judgment of the EU General Court in intel and the so-called 'More Economic Approach' to abuse of dominance,' *World Competition: Law and Economics Review*, **37**(4), 405–434.
World Bank (2021), World Development Report 2021: Data for Better Lives. World Bank Group: Washington. https://www.worldbank.org/en/publication/wdr2021.
Wu, T. (2018), 'The curse of bigness: antitrust in the new gilded age,' Columbia Global Reports, 75. Columbia University: New York.
Wu, T. (2019), 'Blind spot: the attention economy and the law,' *Antitrust Law Journal*, **82**(3), 771–806.
Zott, C., R. Amit and L. Massa (2011), 'The business model: recent developments and future research,' *Journal of Management*, **37**(4), 1019–1042.
Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.