THE INTERSECTION BETWEEN COMPETITION AND DATA PRIVACY

OECD Roundtables on Competition Policy Papers, No. 310

https://doi.org/10.1787/20758677

A joint working paper from the OECD Competition and Digital Economy Policy Secretariat

Carolina Abate, Giuseppe Bianco, Francesca Casalini

OECD

The intersection between competition and data privacy

Carolina Abate, Giuseppe Bianco, Francesca Casalini

Data plays an increasingly important role for online platforms and the majority of digital business models. Along with data becoming central to competition and the conduct of actors in digital markets, there has been an increase in data privacy regulations and enforcement worldwide. The interplay between competition and data privacy has prompted questions about whether data privacy and the collection of consumers' data constitute an antitrust issue. Should competition considerations be factored into decisions by data protection authorities, and, if so, how can synergies between the two policy areas be enhanced and tensions overcome?
This paper explores the links between competition and data privacy, their respective objectives, and how considerations pertaining to one policy area have been, or could be, included into the other. It investigates enforcement interventions and regulatory measures that could foster synergies or lead to potential challenges, and offers insights into models for co-operation between competition and data protection authorities.

This paper is part of the series "OECD Roundtables on Competition Policy Papers", https://doi.org/10.1787/20758677.

Foreword

With the development of the digital economy, data has assumed an increasingly important role for online platforms and most digital business models, often becoming central to the conduct of actors in digital markets and to competition. At the same time, there has been an increase in data privacy regulations and enforcement worldwide.

The intersection between competition and data privacy has recently emerged in the assessments and investigations conducted by various competition agencies. This has prompted questions about whether data privacy and the collection of consumers' data constitute an antitrust issue, whether competition considerations should be factored into decisions by data protection authorities, and, if so, how synergies between the two policy areas can be enhanced and the points of tension be overcome.

This paper explores the interplay between competition and data privacy. It analyses their respective objectives and examines how considerations pertaining to one policy area have been, or could be, included into the other. Furthermore, it investigates enforcement interventions and regulatory measures that could foster synergies or lead to potential challenges. It concludes by offering insights on models for co-operation between competition and data protection authorities.

This paper was prepared by Carolina Abate of the OECD Competition Division, Giuseppe Bianco and Francesca Casalini of the OECD Digital Economy Policy Division. It benefitted from comments by Ori Schwartz and Antonio Capobianco of the OECD Competition Division; Clarisse Girot and Gallia Daor of the OECD Digital Economy Policy Division. It was prepared as a background note for a joint roundtable by the OECD Competition Committee and the OECD Working Party on Data Governance and Privacy on "The Intersection between Competition and Data Privacy" taking place in June 2024, https://www.oecd.org/competition/intersection-between-competition-and-data-privacy.htm. The opinions expressed and the arguments employed in the note do not necessarily reflect the official views of the Organisation or of the governments of its Member Countries.

Table of contents

Boxes

1 Introduction

The widespread "datafication" of social and economic activities has led to an increase in the collection, access and sharing of personal data. This has raised the profile of data privacy concerns and driven a global expansion of privacy and personal data protection laws.[1] In parallel, the concentration of an extensive amount of data in the hands of large digital companies has rapidly become a concern for the resulting market power wielded by such actors, which can potentially lead to anticompetitive conduct and the infringement of users' data privacy.

As a result, there has been increased focus of both data protection and antitrust enforcement authorities on business practices around data. Digital markets affect data privacy because business models often rely on the collection of significant amounts of personal data, which can be used to profile individuals also with regard to sensitive aspects of their private lives, and data protection authorities have started assessing the scope and effectiveness of the legal bases for processing such personal data. The collection, access, and sharing of data have also become increasingly relevant to competition assessments as firms' data practices are a central element of competition dynamics in digital markets, through their role in both strengthening market power and facilitating anticompetitive conduct.

As data protection and competition authorities apply different conceptual frameworks and pursue different public policy objectives, there is growing attention around the concomitant application of the two legal regimes in digital markets, in instances where the "data subject" or "individual" and the "consumer" clearly overlap.

The relation between competition and data privacy laws is multi-faceted. Their interaction can generate synergies and complementarities, as well as tensions and challenges for regulators (Douglas, 2021[1]; Colangelo, 2023[2]). For years, discussions have taken place around whether data privacy and the collection of consumers' data should be an antitrust problem, if competition concerns and considerations around firms' market power should be taken into account by data protection authorities, and what intersections between the two policy areas should be prioritised. For instance, a merger in digital markets could have a significant impact on the amount and detail of personal data collected and processed: thus, both competition and data privacy laws could be at stake.

These discussions have recently reached a higher level, following court decisions and practices around data which place them at the heart of the concerns of regulators and policymakers in both policy domains. At the same time, a growing body of literature (Douglas, 2022[3]; Chen, 2023[4]; Wiedemann, 2023[5]; Colangelo, 2023[2]) highlights a heightened risk of 'regulatory gaming', whereby certain actors might seek to harness data privacy regulations, compliance mechanisms or tools, for exclusionary purposes, raising the question of how to best address such risk from a good public governance perspective.

[1] For the purpose of this paper, the terms "data privacy" and "personal data protection" are used interchangeably, with more precise specifications in Chapter 2, as relevant. The term "data protection authorities" is used to also encompass "privacy enforcement authorities", and "authorities" is intended to include "regulators" and "agencies". Similarly, for the purpose of this paper the terms "competition policy" and "antitrust" are used interchangeably, with specifications where relevant.

There is growing awareness that while data privacy and competition laws are part of a broader regulatory landscape, specific interventions in one policy area can enhance or hinder the goals of the other. Experts and commentators have noted that, to achieve each domains' respective goals, it may be relevant to incorporate into one's assessment factors traditionally falling outside that specific area of intervention, considering, for instance, data privacy as a quality parameter of competition, or examining how a specific privacy requirement or measure may affect market entry. These questions are especially acute where innovative sectors are often based on two-sided digital markets, complex personal data monetisation models, and data scraping practices such as those which underlie machine learning models.

There are currently several initiatives at the national level aimed at addressing this interplay and adapting to this changing reality. For example, a growing number of competition and data protection authorities are joining forces to pursue their regulatory mandates in a coordinated way, through co-operation platforms and forums, Memorandums of Understanding (MOUs), bilateral co-operation on a case-by-case basis, as well as public declarations in which they detail paths leading to stronger collaboration.

With its role as a knowledge hub for data and analysis, platform for best-practice sharing and international co-operation in both disciplines, and its well-established work with existing networks of regulatory co-operation, data protection authorities, and competition authorities, the OECD can support member countries in meeting this cross-regulatory policy challenge. This report and the joint roundtable aim to be a starting point of practical discussions and lay the foundations for further co-operation between these communities in the coming years.

Other policy areas beyond data privacy and competition law are also pivotal for the proper functioning of data-driven markets, namely consumer protection[2], digital security, online safety, and artificial intelligence (AI) policy. These legal frameworks are interconnected, particularly in the context of AI technologies. The past years have seen the development of a regulatory agenda structured around a shared objective of optimising different regulatory frameworks in order to correctly understand the different legal dimensions of data and data practices as a legal object. The optimal articulation of these legal frameworks nevertheless requires considering the connection points existing between each of them. For this purpose, this paper focuses exclusively on the specific intersection between competition and data privacy regulation.

The remainder of this paper is structured as follows: Chapter 2 describes the links between competition policy and data privacy, analysing their respective goals and the way in which considerations pertaining to one policy area have been included in the other. Chapter 3 focuses on interventions that can foster synergies but also lead to tensions, addressing complementarities and potential challenges, while Chapter 4 provides insights on models for co-operation between competition and data privacy authorities. Chapter 5 concludes.

[2] For example, the Italian competition authority (Autorità Garante della Concorrenza e del Mercato) – which is also the consumer protection authority – has found violations of the Consumer Code for practices related to the collection and processing of consumers' data for commercial purposes and issued fines against Google and Apple (Autorità Garante della Concorrenza e del Mercato, 2021[95]).

2 The growing linkages between competition and data privacy

2.1. The goals of competition law and data privacy law

Competition law and data privacy laws share "family ties", as both pursue an overarching objective of protecting the welfare of the individual, whether as a consumer or as a data subject. They also share the policy objective, directly or indirectly, of addressing the power asymmetry between firms, or organisations, and individuals (Botta and Wiedemann, 2019[6]). Whereas this may be more evident for competition law, data privacy law is concerned with them in terms of information and power asymmetries that may prevent individuals from controlling their personal data (Costa-Cabral and Lynskey, 2017[7])).

In this respect, the objectives and concerns also align with those of consumer law, for example with regard to addressing unfair contractual terms (e.g. (UK, 2015[8])). However, despite these common features between competition and data privacy laws, the scopes, goals, conceptual frameworks, and procedures of the two policy areas differ significantly.

2.1.1. Competition law

Competition law applies to all entities that engage in economic activity. Its main goal is to maintain and encourage the process of competition, promoting the efficient use of resources while protecting the freedom of economic action of various market participants (OECD, 2003[9]). Its enforcement mechanisms, which vary across jurisdictions, aim at ensuring that companies compete on their merits and at avoiding economic harm, i.e. a negative impact on variables such as price, quality, choice or innovation (Costa-Cabral and Lynskey, 2017[7]).

The goal of competition policy is to ensure that companies' conduct, whether unilateral, coordinated, or resulting from a merger, does not hinder any economic aspect of consumer welfare (or general economic welfare) and the competitive process. Thus, competition policy protects a "public interest" in competitive markets, while dealing with rights of individuals only indirectly, differently from data privacy policy.

Although various standards exist for competition law, each with its advantages and disadvantages, the consumer welfare standard currently stands as the predominant standard worldwide. Despite its widespread use, this standard is still the focus of an ongoing debate on whether it is interpreted too narrowly. However, as under most other welfare standards, factors beyond price can be considered when assessing anticompetitive behaviour (for an in-depth discussion on standards see (OECD, 2023[10])).

Therefore, while competition authorities are concerned with firms' anti-competitive behaviour, within their mandate they can take into account a diverse set of factors that affect markets, if these are important elements of consumer welfare and could signal harm. This includes scenarios where prices may not be the most relevant parameter of competition, typically in digital markets (see also (OECD, 2018[11])). Section 2.2 below analyses in more detail whether and how competition authorities have integrated data privacy considerations in their assessments and decisions.

2.1.2. Privacy and data protection laws

The discussion of privacy as a right gained prominence in Europe and the United States towards the end of the 19th century. Privacy is a difficult concept to define, as it is used in a variety of legal contexts (Solove, 2006[12]) and hinges on the balancing of public and private spheres between individuals, organisations, and governments (Acquisti, Curtis and Liad, 2016[13]). In Europe, the experience of the abuse of personal data to control citizens and persecute some groups or individuals has forged the right to privacy, which has been deemed a form of protection of human dignity (Waxman, 2018[14]). Conversely, in the United States the concept of privacy is rooted in the safeguarding of liberty vis-à-vis the State (Whitman, 2004[15]). At the international level, the human right to privacy is protected under Article 12 of the UDHR[3] and Article 17 of the ICCPR[4] (UN General Assembly, 1948[16]; UN General Assembly, 1966[17]).

Throughout the years, technological advancements have played a pivotal role in shaping the concept and the public expectations around privacy (OECD, 2024[18]). The advent of printing and photography enabled the recording, dissemination and capture of information that would have previously been limited to a small circle (CNIL, 2021[19]).The rise of information and communication technologies (ICTs) and large electronic databases in the 1960s raised new and important challenges: personal data could be processed with computers and could be stored, compared, linked, selected and accessed in unprecedented ways, by thousands of users at geographically dispersed locations and pooled with the creation of complex national and international data networks (OECD, 2023[20]). As a consequence, legislations started recognising more specific legal rights for data subjects regarding their personal data.

The OECD was at the centre of international discussions on these technological developments. In that context, negotiations led to the adoption of the OECD Privacy Guidelines – the first internationally agreed-upon set of privacy principles – in 1980. Subsequent work further explicitly highlighted the importance of establishing and maintaining privacy enforcement authorities to ensure effective application and supervision of privacy laws (OECD, 2013[21]).

While the OECD Privacy Guidelines are widely deemed as the global minimum standard for privacy protection, specific privacy and personal data protection legislations vary considerably across jurisdictions. They are generally aimed at the protection of individual rights or interests. Depending on the jurisdiction, privacy and personal data protection can be a constitutionally protected right (e.g. in several European countries, and under the notion of "*habeas data*" in Latin America), framed in terms of consumer protection law (at the US federal level), or conceived primarily in terms of legally binding principles (e.g. in Australia and Canada) (Douglas, 2021[1]). While the right to privacy applies to a broader set of issues than the electronic processing of personal data, the part of privacy law most relevant for the present analysis is personal data privacy law, i.e., the area of privacy law that deals specifically with the protection of individuals' personal data.

The scope of application of personal data protection laws is determined by the concept of "personal data", which is commonly understood in legislations like EU GDPR as any information related to an identified or identifiable natural person, although on this threshold there is also variation among jurisdictions (Botta and Wiedemann, 2019[6]). For privacy law, data subjects can be consumers but also individuals when interacting with public bodies: privacy law applies to all bodies that collect or process personal data, regardless of whether these bodies are engaged in market activities.

[3] Article 12 UDHR provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (UN General Assembly, 1948[16]).

[4] Article 17 ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation" and that "everyone has the right to the protection of the law against such interference or attacks" (UN General Assembly, 1966[17]).

Depending on the jurisdiction, privacy enforcement authorities have a set of powers ranging from investigations into processing operations, ordering the notification of personal data breaches, imposing bans on processing or administrative fines, and referring matters to a court. Personal data are often managed through "complex arrangements involving a network of data controllers (namely, those who keep, control, or use personal data) and subcontractors and service providers operating globally" (OECD, 2011[22]),.

This complexity has long challenged the traditional territorial approach to data protection (OECD, 2011[22]), with the consequence that the same data processing operation is frequently subject to the cumulative application of several laws. At the same time, privacy enforcement authorities have a mandate limited to the specific rights, interests or principles recognised in their jurisdiction, and they are not necessarily required, or have competence, to assess market conditions or other economic factors, differently from competition authorities.

2.1.3. Digital ecosystems: an intersecting area to regulate

Despite these fundamental differences in origins, data-driven digital markets and the rise of complex digital ecosystems increasingly show a significant intersection between competition and data privacy policy interests. This interplay influences economic activities and firms' market conduct more broadly.

Digital ecosystems rely on the processing of personal data as a key element of their business model and as a source of market power, risking in some specific instances blurring the lines between competition authorities' and data privacy authorities' areas of competence. A relevant example is that of the ad tech market. In this respect, data protection authorities in the EU have considered the application of data protection principles, including the lawful bases to the processing of data for personalised services and behavioural advertising (see for example (Irish Data Protection Commission, 2022[23]; 2022[24]; OECD, 2020[25]), whilst competition authorities have considered abuse of dominance matters by reference to privacy quality offered (Bundeskartellamt, 2019[26]).

Consequently, data protection authorities – traditionally not viewed as economic regulators – find themselves evaluating market offerings that vary in price and in the level of personal data profiling involved. This situation arises for example in what is referred to as the "pay or consent" model, wherein considerations include the company's market position, the presence of lock-in or network effects, the adequacy of fees proposed by companies (EDPB, 2024[27]), all factors more commonly addressed in competition enforcement. In parallel, competition authorities find themselves engaged in evaluating the privacy policies of companies, which is a task more commonly seen as a data protection authorities' prerogative.

In circumstances where competition enforcement can have an impact on how data are collected, used or transferred, data privacy becomes a necessary consideration. Similarly, when data privacy regulation is applied to highly concentrated markets where data are used to maintain, enhance, and potentially abuse, market power, antitrust inevitably is an element for consideration and provides a relevant frame of reference. These dynamics underscore the importance of dialogue and collaboration between the two communities, based on sharing expertise and analysis of fast-evolving digital markets, and of the technologies which underlie them.

2.2. Is data privacy an antitrust concern?

The question of whether competition policy should concern itself with issues and considerations stemming from other policy areas has long been debated. Historically, competition authorities tended to exclude data protection and privacy considerations from their assessments, as they were seen as standalone elements and deemed to fall outside of the scope of competition. This perspective aligns with the more economic

approach, according to which the only goal of competition law should be to promote consumer welfare (or the relevant welfare standard), measured in economic terms of price and quality increase or decrease, and consumer choice.

In the US, the question of whether data privacy should be a concern within antitrust started to emerge over a decade ago, in the context of the *Google/DoubleClick*[5] merger in 2007 and of Microsoft's offer for acquiring Yahoo in 2008. Despite not being followed upon as a realistic harm to competition, in both cases the need to scrutinise the potential adverse effect on consumers' data privacy was debated (Lande, 2008[28]).

For instance, in *Google/DoubleClick*, data privacy concerns were raised in particular by the Electronic Privacy Information Center (EPIC). The US Federal Trade Commission (FTC) rejected the idea that data privacy considerations could be taken into account in a merger analysis, noting that not only the FTC lacked legal authority to intervene imposing conditions not related to antitrust, but also that "regulating the privacy requirements of just one company could itself pose a serious detriment to competition"[6] in a rapidly evolving industry (Ohlhausen and Okuliar, 2015[29]).

In 2014, consumer groups and privacy advocates voiced similar concerns around data privacy following the proposed transactions *Facebook/Whatsapp*[7][8] and *Google/Nest Labs*[9], without consequences for the competitive assessment of the acquisitions. This mirrored the US regulators' approach in the late 2000s, which have traditionally interpreted matters around data privacy and platforms' misuse of data as being exclusively within the scope of consumer protection authorities, and fully outside the mandate of antitrust regulators (Akman et al., 2022[30]).

In Europe, in the context of the European Commission's (EC) case *Asnef-Equifax*[10], the Court of Justice noted in its judgement from November 2006 that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection"[11]. In the following years, similar references to the applicability of data privacy laws, and to the importance of the separation between these and competition law, were made in a number of EC decisions, such as *Google/DoubleClick*[12] in 2008, where the EC emphasised the separate applicability of privacy and data protection laws, and thus of the obligations to be imposed onto the merged entity, in particular with regard to the processing of personal data.

In 2014, in the *Facebook/WhatsApp*[13] decision, the Commission reinforced the idea that any data privacy-related concerns emerging from the concentration and accumulation of data in the hands of the merged entity do not fall within the scope of competition law but within the scope of EU data protection rules.

---

[5] FTC Filed No. 071-0170

[6] Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007).

[7] See also https://epic.org/wp-content/uploads/privacy/internet/ftc/whatsapp/FTC-facebook-whatsapp-ltr.pdf

[8] https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed-acquisition

[9] Fed. Trade Comm'n, Early Termination Notices, 200140457: Nest Labs, Inc., and Google, Inc., (Feb. 4, 2014), http://www.ftc.gov/enforcement/premerger-notification-program/early-termination-notices/20140457

[10] Case C-238/05

[11] https://curia.europa.eu/juris/showPdf.jsf?text=&docid=65421&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=40586

[12] Case COMP/M.4731

[13] Case COMP/M.7217

Similarly, the 2017 *Microsoft/LinkedIn*[14] Commission decision served as a reminder that the risks associated with data combination strategies would be mitigated and addressed by the applicable data privacy rules.

Until recently, the Competition Bureau of Canada had also been clear that its mandate would not extend to data privacy concerns unrelated to competition, in that competition law and data privacy law relate to different rights and focus on different harms, thus sharing the US's and EU's "separatist perspective" (Akman et al., 2022[30]). However, the current comprehensive review and modernisation of the competition regime, which aims, amongst other things, at better addressing potential competition issues in digital markets, revealed an initial shift. The June 2022 amendments[15] to the Competition Act determined that, when assessing the effect of potentially anticompetitive practices on competition, the Competition Tribunal may consider the impact on both price and non-price competition, including quality, choice or consumer privacy.

Despite this historical inclination to keep competition law and data privacy as two separate realms, certain jurisdictions are now viewing the collection and sharing of consumer data as a concern relevant for competition policy and enforcement, as data privacy goes from being seen exclusively as a separate standalone variable to potentially constitute a component of quality, on which companies can compete. This shift reflects emerging considerations around the concepts of quality and consumer choice, and what these entail in digital markets. In particular, when consumers and users are also data subjects, and data play a pivotal role in platforms' market power, data privacy could become a relevant non-price parameter of competition, whether as a dimension of quality or of choice.

More specifically, the analysis of digital markets has uncovered the flaws of the notion that emphasising price effects alone, thus ensuring effective price competition, would naturally address other dimensions of competition (Lande, 2008[28]). Indeed, digital markets' business models and dynamics show that this is not necessarily the case, as there are situations where, if certain non-price parameters, such as data privacy, are not explicitly considered, there is a potential risk of harming competition on that specific parameter.

In their 2016 joint report on competition law and data, the French and German competition authorities state that a strong link between a firm's dominance, its data processes, and competition, "could justify the consideration of privacy policies and regulations in competition proceedings". Indeed, as companies' data-related decisions can have implications on competition, "privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services" (Autorité de la concurrence; Bundeskartellamt, 2016[31]).

On this basis, an "integrationist approach" is emerging, posing that data privacy has a role to play in competition assessments, as a non-price parameter of competition that can affect consumer welfare (see also (Górecka, 2022[32]; Douglas, 2021[33]; Chen, 2023[4])). In particular, in markets where companies compete on the level of data protection that they provide to consumers, an analysis of the potential harm to competition deriving from a firm's conduct or a merger should also include an examination of data privacy-based competition. For instance, a firm with strong market power over its end users might harm consumer welfare through data privacy degradation, where data privacy is seen as an element of quality, or the firm might also exploit data privacy laws to abuse its market power. Section 2.2.1 below will further illustrate a number of theories of harm related to data privacy.

[14] Case COMP/M.8124

[15] Part of the *Budget Implementation Act, 2022, No. 1.* *Bill C-19 441 An Act to implement certain provisions of the budget tabled in Parliament on April 7, 2022 and other measures | Projet de loi C-19 441 Loi portant exécution de certaines dispositions du budget déposé au Parlement le 7 avril 2022 et mettant en œuvre d'autres mesures*

Moreover, even when companies do not directly compete on data privacy but build their business models and their market power on the accumulation, combination and processing of data, thus making data an essential factor to compete, a company's handling of such data becomes a concern not only for data protection authorities, but also for competition authorities (Stauber, 2019[34]). In turn, this implies that competition authorities' interventions in data-driven markets can influence data privacy, while the activities of data protection authorities can enhance or hamper competition. Chapter 3will analyse in depth the complementarities and tensions between these two policy areas.

In recent years, there has been a noticeable shift among competition authorities towards recognising data as a key input and a source of competitive advantage, with a focus on data-related theories of harm (see (OECD, 2023[35]). However, this trend has not clearly extended to data privacy itself, which has yet to receive extensive consideration in competition authorities' assessments. While there are indications of growing openness towards the idea of including data privacy concerns in antitrust discussions, this remains largely theoretical and has not yet translated into enforcement practices.

One exception, which may foreshadow a more substantial shift in competition authorities' treatment of data privacy in the future, is the Bundeskartellamt approach in its well-known case against Facebook (the *Meta Platforms* case)[16], opened in 2016, as well as the following preliminary ruling by the Court of Justice of the EU (CJEU) in July 2023[17]. In addition to establishing that a competition authority may take into account data protection regulations in the context of its competition investigations, the CJEU also acknowledged that accessing and processing personal data has become a significant parameter of competition and thus excluding such considerations from competition assessments "would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union". Box 2.1 below describes the case in more detail.

Box 2.1. The *Meta Platforms* case

In 2019, the Bundeskartellamt issued a decision against Facebook (now Meta) for excessive collection of users' data, which constitutes an abuse of its dominant position on the market for online social networks for private users in Germany, under Section 19(1) of the German Competition Act.

The decision prohibited Facebook from making the use of the social network conditional on the collection of user data from third-party websites and other services owned by Facebook, and on the combination of such data with those collected though the social network, in that the inclusion of such conditions in Facebook's terms of service constituted an exploitative abuse.

This combination of data was carried out by Facebook via Facebook Business Tools, which website operators, developers, advertisers and other businesses integrate into their own websites or apps via APIs (Application Programming Interfaces) predefined by Facebook in the form of "Like" or "Share" buttons, without the users' consent.

To reach its finding of a breach of competition law, the Bundeskartellamt considered – upon consulting the relevant data protection authority – that Facebook's data processing policies were imposed on users in violation of the European data protection rules, to the detriment of users, and could not be justified under Article 6(1) and Article 9(2) of the GDPR. The data privacy laws violation was deemed to be a

[16] Case B6-22/16, Bundeskartellamt (6th Division) decision from 6 February 2019, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6- 22-16.pdf .

[17] Meta vs Bundeskartellamt Case C-252/21, judgement of the Court from 4 July 2023, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1652408 .

manifestation of Facebook's market power. In addition, it was found that, through this unlawful data processing, Facebook would strengthen its competitive data advantage over competitors, increase barriers to entry, and ultimately impede competition.

As highlighted in Botta and Wiedemann (2019) the violation of data privacy laws is a key element of the Bundeskartellamt's decision to find Facebook's conduct abusive. Due to this special interplay between privacy and antitrust considerations, throughout the investigation the Bundeskartellamt consulted and cooperated with data protection authorities (in the German federal system and in the EU), none of which claimed to have exclusive competence[18]. The Bundeskartellamt further clarified in its background information to the decision that, "where access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is not only relevant for data protection authorities, but also for competition authorities" (Bundeskartellamt, 2019).

After an appeal to the Düsseldorf Higher Regional Court, which questioned the Bundeskartellamt's authority to enforce data protection rules under antitrust laws and suspended the effects of the 2019 ruling, the Bundeskartellamt's approach was confirmed by the German Federal Court of Justice, which overturned the previous appeal, and more recently by a preliminary ruling by the Court of Justice of the European Union[19].

In its 2023 judgement, the CJEU clarified that, when assessing an abuse of dominant position, competition authorities can also take into consideration, on the basis of all circumstances of the case, rules other than those relating to competition law, including the GDPR, without prejudice to the powers conferred on the relevant supervisory authorities. The CJEU held that "the compliance or non-compliance of th[e company's] conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers"[20].

In addition, the duty of sincere co-operation, enshrined in Article 4(3) of the Treaty on the European Union, implies that competition authorities have to consult and seek the co-operation of data protection authorities. Therefore, it was found, competition authorities can find a breach of the GDPR, after consulting data protection authorities, when this is necessary to establish an abuse of dominant position.

Sources:
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", Antitrust Bulletin, pp. 428-446;
Bundeskartellamt (2019), Background information on the Bundeskartellamt's Facebook proceeding, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6.

A similar approach emerges from the Competition Commission of India (CCI)'s investigation[21] into WhatsApp's privacy policy ("WhatsApp Privacy Policy Case"), started in 2021 for an alleged violation of Section 4 of the Competition Act. The investigation aimed at determining whether WhatsApp was abusing

[18] Case summary https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

[19] The Düsseldorf Higher Regional Court which has to decide on the merits, being bounded to follow the German Federal Court, decided to stay proceedings and make a reference for a preliminary ruling to the CJEU.

[20] Meta vs Bundeskartellamt Case C-252/21, judgement of the Court from 4 July 2023, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1652408 .

[21] Suo Moto Case No. 01 of 2021 2021.03.24 (Suo Moto - direction to investigate).pdf - Google Drive

its dominant position by imposing unfair conditions upon users, through its privacy policy's data sharing terms. WhatsApp and Facebook filed a petition in the Delhi High Court[22] against CCI's decision to investigate, one of the reasons being that the 2021 policy under investigation fell under the purview of the information technology law framework and the issues at stake were overlapping. The High Court confirmed that there were sufficient reasons to investigate this case under competition law, due to the competition concerns around data collection and usage (see also (Pal and Kumar, 2021[36])).

2.2.1. Theories of harm

In competition investigations, different theories of harm built around data and data privacy can be envisaged. Broadly, in abuse of dominance cases, these are generally articulated in terms of exclusionary and exploitative effects, within the limits of the jurisdiction's legislative framework. However, in the case of data privacy-related theories, this distinction is not always clear-cut, as conducts can often lead to both types of effects simultaneously.

The main category of exploitative abuses relates to data privacy degradation, where data privacy is seen as a non-price parameter of competition and the weaker data privacy protection offered to users as a reduction in quality. The decrease in quality, resulting from the lower data privacy offered to consumers, can also be interpreted as an increase in the quality-adjusted price of the service (Kemp, 2020[37]), and platforms can carry out this conduct in different ways. It is important to note that the risks related to data privacy degradation can also emerge as the result of a merger, in particular if the merging entities were previously competing on the level of data privacy offered.

The Bunderskartellamt decision against Meta, described in Box 2.1 above, exemplifies the case of excessive collection of users' data from third-party sources as exploitative abuse. Indeed, a firm with strong market power over its end users, whose business model relies on collecting and processing users' data, may have the incentive to reduce the level of data privacy offered to users, and increase data collection to a level that is excessive or unfair, taking advantage of its position to the detriment of consumers.

Excessive data collection can be appraised as a form of the more traditional excessive prices theory of harm, accepting the analogy of data as "the currency of the digital age" (see (Robertson, 2020[38]), (Stucke, 2018[39])), or as the imposition of unfair terms and conditions. The comprehensive debate around establishing what constitutes fairness or excessiveness (which can be informed by parameters such as users' reasonable expectations, the parties' bargaining power, principles of proportionality and equity, or the indispensability of a trading condition (Robertson, 2020[38])) is beyond the scope of this chapter.

Another example of how data privacy degradation could take place pertains to so-called concealed data practices. As defined in (Kemp, 2020[37]), concealed data practices occur "when suppliers' terms provide weak privacy protections for consumers while the extent of those terms, the resultant data practices and the consequences of these data practices are concealed from consumers", leading to "the collection, retention, use and/or disclosure of personal information, beyond that which is necessary for the provision of the service in question and beyond the reasonable expectations of the consumer", with potential cascade effects in several markets. In addition to being detrimental for consumers (or exploitative), these practices also undermine the competitive process by further strengthening the platform's market power, increasing barriers to entry and hampering data privacy-enhancing rivals' ability to compete.

Indeed, the exploitation through concealed practices allows the dominant company to accumulate and combine data in a way that is not easily replicable by competitors and that can be monetised on the advertisers' side of the market. This provides an unfair competitive advantage to the platform over those rivals who are data privacy compliant, on both sides of the market. Moreover, as highlighted in (Kemp, 2020[37]), due to the concealed nature of these practices, "consumers cannot place a value on the improved

[22] WhatsApp v CCI - Del HC - DB Order 25.08.2022.pdf - Google Drive

privacy quality offered by a rival when they cannot make any real comparison between the privacy terms and practices of the incumbent and its rivals"(…). "Privacy-enhancing rivals are therefore impeded in their ability to compete on privacy quality because the nature and extent of the detriment caused by their rivals' privacy-degrading practices is hidden by the combined effect of concealed data practices and the lack of implied quality information in zero-price markets".

Similarly, other types of conduct can have both exploitative and exclusionary effects. This is the case of privacy policy tying. In the broader context of envelopment strategies[23], privacy policy tying can be defined as a strategy through which a dominant conglomerate platform can condition the provision of services in one market to the acceptance of a privacy policy that allows bundling of user data across all services in unrelated markets. Acquiring data from a secondary market, and extracting user's consent to the combination of its data across markets, would allow the platform to monetise the combined data, and obtain an insurmountable data advantage in the origin market, reinforcing the platform's market power there and protecting it from new entrants. Thus, under this theory, the potential exclusionary effects may be accompanied by an exploitative abuse, in the form of the coercive tying of privacy policies (Condorelli and Padilla, 2020[40]; 2023[41]).

Finally, purely exclusionary abuse type of theories can also be relevant for merger control (see also (OECD, 2023[35])). These theories, such as input foreclosure (where the input is data), are generally built around companies' use of data more than data privacy considerations as such (OECD, 2020[42]). However, in these cases, the remedies that may be imposed can affect data privacy, revealing potential conflicts between solutions that promote competition and those that protect personal data.

This holds true for theories of harm reflecting concerns around large platforms' accumulation and combination of data, which have emerged in merger cases, articulated as both horizontal and non-horizontal at various times. By combining datasets, the merging firms can entrench their market power, thereby raising entry barriers and costs for competitors. This aspect will be further explored in Chapter 3.

While most of these theories remain untested, especially those more closely related to data privacy, and are not part of the current enforcement practice, they bring to light a series of elements indicating the potential relevance of data privacy considerations for the work of competition authorities in digital markets.

2.3. Is competition a data privacy law concern?

The extent to which competition should or can be a data privacy law concern raises questions that are different from the extent to which data privacy can be a competition concern. Data privacy laws provide specific rights for individuals and obligations for individuals and organisations, but do not directly envisage guardrails for the market as a whole. As such, data privacy enforcement is only partially receptive to exogenous (in this case, competition-related) considerations that are not envisaged in the data privacy framework of reference. This stands in contrast to competition authorities that traditionally have broad responsibilities over the functioning of markets and are thus amenable to the inclusion of various, diverse considerations in their assessments.

In essence, while it may be conceptually straightforward to include data privacy as a quality parameter in competition assessments, as demonstrated by the recent jurisprudence that addresses this point and presented in the previous section, establishing the reverse relationship can be more challenging.

Against this background, the answer to the question "is competition a data privacy law concern?" might be approached along two distinct axes. Firstly, it may be done by considering the theoretical avenues through

[23] As defined in (Eisenmann, Parker and Van Alstyne, 2011[90]), "envelopment entails entry by one platform provider into another's market by bundling its own platform's functionality with that of the target's so as to leverage shared user relationships and common components".

which competition considerations could support and bolster privacy and data protection enforcement actions, a scenario that however currently remains hypothetical. Secondly, another option may be to examine the ways in which data privacy policymakers and regulators are beginning to look at competition policy functions and insights to support and enhance their own policy objectives and regulatory outcomes beyond specific enforcement actions.

2.3.1. Integrating competition analysis into data privacy enforcement

Traditionally, data privacy laws seek to implement data subjects' rights with limited consideration for market power or market dynamics. Nevertheless, the notion of imbalance between data subject and controller, which exists in some data privacy regulations, may provide a basis to consider a firm's market position in the context of privacy and personal data protection enforcement.

In theory, data protection authorities could approach enforcement considering the size or market position of a company to scale expectations regarding compliance, in cases of more prescriptive approaches to data privacy protection, or to evaluate the gravity of identified harms to individuals in cases of *ex post* enforcement approaches to data privacy regulation. In other words, it could be envisaged that dominant or large firms should be subject to reinforced accountability obligations proportionate to the risks which they generate compared with non-dominant or smaller firms regarding data privacy. In this context, concepts such as market definition, market power, and special responsibility, all of which are common in competition law, could serve as relevant interpretive tools for data protection authorities (Graef, Clifford and Valcke, 2018[43]). On the other hand, in the long run, this may have the effect of further pushing users to opt for large firms, if users become aware that these firms offer higher standards of data privacy and act upon such awareness.

In the EU, Recital 43 of the GDPR provides that consent should not serve as a valid legal ground for processing personal data in cases where there is "a clear imbalance" between the data subject and the controller. The Court of Justice of the European Union has noted that "as a matter of principle, the fact that an online social network holds a dominant position does not prevent users from validly giving their consent" (Court of Justice of the European Union, 2023[44]). At the same time, the European Data Protection Supervisor (EDPS) has pointed out that "where there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory" (EDPS, 2014[45]).

This latter perspective is also highlighted in the context of enforcement remedies, particularly fines. According to the European Data Protection Board (EDPB) Guidelines, a data protection authority may place greater emphasis on the nature of the processing when there is a clear imbalance between data subjects and the controller (EDPB, 2023[46]).[24]

Similarly, the UK Information Commissioner's Office (ICO) Data Protection Fining Guidance states that, when evaluating the severity of an infringement, particularly with regard to the nature of the processing, it will consider this factor to be more significant in cases of clear power imbalance between data subjects and controllers – and it provides a specific note that this "includes where the imbalance arises from the market position of the controller" (ICO, 2024[47]). The guidance, while not explicitly establishing enforcement priorities, provides valuable insights into the areas that the ICO deems most serious and, consequently, where it is most likely to commence action (Fara and Moss, 2023[48]).

As a matter of fact, currently, "when determining data controllers' obligations under the GDPR, only limited weight is given to their market power, and DPAs do not assess whether a market is competitive enough for consumers to have a real choice" (D'Amico, 2023[49]). No relevant jurisprudence seems to exist outside

[24] It should be noted that the examples provided by the EDPB Guidelines do not refer to imbalance in the competition sense, but it does not indicate the list to be exhaustive either: "when there is a clear imbalance between the data subjects and the controller (e.g., when the data subjects are employees, pupils or patients)" (EDPB, 2023, p. 18[46]).

of the GDPR bloc, either. In addition, data protection authorities have so far steered clear of defining what a higher responsibility might imply, an approach that may potentially be detrimental to objectives of legal certainty and transparency.

Furthermore, some authorities may refuse the notion of scaling data privacy obligations to market power as a matter of theory or do so only indirectly through the way in which they prioritise enforcement action. This is the case of the French data protection authority: in response to empirical studies highlighting the tendency of the GDPR to favour large players, it stated that it intends to increasingly take an "asymmetric dimension to its regulatory action on digital markets" (CNIL, 2024[50]).

To the extent that competition is a relevant factor in order to assess dominance in a given market and related data privacy issues, it has been suggested that data protection authorities could – after consulting the competition authorities – rely on their opinions or on competition authorities' previous decisions, as well as on other *ex ante* evaluations or assessments (e.g. the list of gatekeepers under the Digital Markets Act (DMA) (D'Amico, 2023[49])) or firms designated as having strategic market status under the UK's proposed Digital Markets, Competition and Consumers Bill (UK Parliament, 2023[51])) to determine data privacy questions.

2.3.2. Leveraging competition policy concepts to support and enhance data privacy regulatory outcomes

Along the second axis of the question, data privacy policymakers and enforcement authorities are increasingly confronted with competition-related questions in their roles. There is a growing interest in understanding how competition dynamics may factor into (or "are a concern for") data privacy regulatory outcomes as an underlying, relevant, structural premise.

A key question relates to how data policymakers can foster the development of data privacy as a competitive advantage. If competitive markets tended towards increased data privacy as a parameter of increased quality, it could be envisaged that greater competition would result in greater quality/privacy offerings. In essence, data protection authorities may be concerned with competition as a foundational mechanism for improving data privacy outcomes.

For example, it could be argued that insufficient competition would hinder individual data privacy rights or principles such as the right to erasure or the right to access. These rights might suffer if authorities lack reference to other companies' behaviour that they may use as benchmarks to demonstrate how these rights should be meaningfully ensured. In practice, laws do not generally specify a precise time frame allowed for processing an individual's request for their data to be erased or transferred to them (for example, Article 17 of GDPR uses the expression "without undue delay"). The rationale for this flexible language is to provide some reasonable and legitimate leeway to organisations in complying with data privacy laws. In these contexts, where there is no precise data privacy obligation set *ex ante* by the legislative framework, authorities will reasonably be influenced by data practices observed in the market in their determinations, and the absence of competition may result in lower overall quality/privacy standards.

Similarly, the principle according to which data subjects should be able to withdraw their consent without detriment[25], recognised by some data privacy laws, could be affected in the absence of competition in the market. This could be a most clear case when there is a justified monopoly whereby an individual cannot refuse or withdraw consent without detriment due to a lack of alternative of that infrastructural service provision.

[25] See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12

Some have alleged that this issue is somewhat relevant in discussions surrounding the emerging 'pay or consent' model proposed by firms that hold significant market power. In those cases, they argue that that the detriment to consumers arises from the requirement to pay for the service in the absence of consent to provide data, thereby facing the negative consequence of having to pay given that there are no existing competitors (Datatilsynet, 2024[52]). As the case may be, there might be a correlation between level of competition in the market and potential detriment to users when refusing consent, and data protection authorities will have to determine whether and how to address this correlation.

A sub-issue of the above relates to what incentives policymakers and regulators could provide to support the development of a competitive market for privacy-enhancing technologies (PETs) (OECD, 2023[53]). In fact, the lack of effective competition is currently considered to be one of the factors hindering the development and diffusion of privacy-enhancing products, whose maturity is growing fast, as large digital incumbents do not have strong incentives to accelerate the use of PETs and it is costly and complex for smaller market entrants to think of competing with dominant firms by using more privacy-friendly practices. This may be seen as leading to an overall detriment of the principle of “privacy by design”. In other cases, PETs are sometimes implemented by large technology companies to expand their dominance in digital markets (Ranieris, 2021[54]), also leading to negative implications for competition.

Against this background, data protection authorities have been growing interested in understanding the dynamics of digital markets, to be able to achieve better regulatory outcomes. They seek to gather new economic insights to inform their recommendations and their enforcement actions, to assess both the impact of competitive dynamics on data privacy and the impact of data protection authorities’ action on markets more broadly. The French DPA has created an economic analysis team (CNIL, 2023[55]), whereas the Italian DPA has undertaken an enquiry into Big Data with the Competition and the Communications Authorities (Garante, 2019[56]). The UK ICO started building its economics team in 2020. It published an Impact Assessment Framework to ensure that regulatory action is both proportionate to the issue at hand and not unduly burdensome on those that they regulate, so that the regulator can balance different obligations and objectives including economic growth (ICO, 2023[57]).

3 Complementarities and potential challenges

The interaction between competition law and data privacy law is generally analysed under four scenarios reflecting the possibility that a specific conduct or intervention could be in compliance with one legislative framework and not the other, or both, or neither (Carugati, 2021[58]). For instance, in the recent *Meta Platforms* case (described in Box 2.1) the German competition authority argued that Meta's conduct not only breached data privacy law, but also constituted an abuse of dominant position under competition law. Thus, the enforcement of competition law could benefit data privacy law, and vice versa.

Other cases might find the enforcement of one legislative framework detrimental to the goals of the other. This can happen either when the conduct is in compliance with both legislative frameworks, or when it is in violation of one of the laws. In the latter situation, the strict non-compliance with a body of law can provide a frame of reference and allow regulators to navigate the interplay between competition and data privacy more easily.

In the case of merger control, for example, if the merging parties are prohibited by data privacy law from combining certain data sources, or from using an acquired data source in a particular way that might otherwise give them an anti-competitive advantage, competition authorities could take this into account when addressing their concerns with the transaction. However, questions might arise as to the appropriateness of taking compliance at face value, especially if there is a track record of insufficient enforcement or of a company's non-compliance with data privacy law.

Within the context of compliance with both regulatory areas, while the intersection between competition and data privacy might show complementarities and mutual influences, the opposite might also be true. In this grey area, divergences might be most difficult to address, since the tensions that can arise do so when measures introduced by one area may be detrimental to the goals of the other while still not infringing the law. Thus, there is no infringement under one legal regime to provide a yardstick.

The cross-border or international dimension adds a further layer of complexity. The same conduct (or business model) of a company that operates in different countries may be deemed to be compliant respectively with competition and/or data privacy regulations and to be not compliant with either (or both) in other jurisdictions. In other words, the four scenarios sketched above multiply by the number of jurisdictions in which the company operates and whose authorities may make an assessment on the company's conduct.

Moreover, the distinction between complementary and divergent interventions is far from being clear and defined, as some measures can be beneficial for both legal regimes in certain cases while being harmful to one of them under other circumstances. This can be seen for example with remedies applied in antitrust cases, conditions applied to clear a merger, as well as with the recent provisions applicable under *ex ante* regimes to regulate digital markets, such as in the Digital Markets Act in the EU.

Similarly, data protection authorities can require the notification of breaches to affected data subjects, which can have a beneficial impact also on competition. As consumers are provided useful information to help them decide whether to continue using the affected services, this can strengthen competition on data

privacy as a non-price parameter, and this effect can be further strengthened by litigation by data subjects (MacLachlan, 2024[59]). Furthermore, when a data protection authority imposes a ban on the processing of personal data, this can help prevent a company from gaining a competitive advantage through unlawfully collected data (FTC, 2021[60]).

At the same time, while data privacy laws enhance the protection afforded to individuals, the risk exists that they can also produce (unintended) adverse effects on competition by strengthening the position of large digital incumbents. For instance, this could be the case with more recent obligations around companies' use of data, which might limit certain firms' ability to compete or enter a market, while benefitting incumbents, which have already been able to build up extensive data sets before regulation was in force or exploiting legal grey areas.

This is particularly relevant for first movers in the development of generative AI, which may enjoy a competitive advantage over other firms. Data privacy laws limit the ability of companies to draw on much of the internet's production of natural language content for other purposes than originally intended, such as for training generative AI models. As first mover companies have been able to train their models in legally grey areas, then, the current data protection authorities' and other authorities' focus on data privacy practices of companies engaged in generative AI may structurally prevent competition in a market where the scale of the database is a key parameter for the final quality of the service offered. However, this is still uncertain, as relevant factors to be assessed include economies of scale, economies of scope, and feedback effects, whose influence may in turn be disrupted by innovation, community collaboration, and emerging technologies (Competition and Markets Authority, 2023[61]).

3.1. Data-related measures

A first example of intervention with potential complementarities but also risks of divergent effects on competition and data privacy pertains to data portability. Data portability is understood as the ability of users to request that a data holder transfer, to them or to a third party, data about them in a structured, commonly used and machine-readable format (OECD, 2021[62]). Data portability is an application of the individual participation principle of the OECD Privacy Guidelines[26]: it gives data subjects control over their data and choice over its use and reuse. It is further enshrined (e.g. in the EU[27], California[28], Brazil[29]) or being considered (e.g. in Canada[30]) in several data privacy regulations as a right of data subjects, while it is also used, in certain circumstances, as a competition-enhancing measure.

As explained in (OECD, 2023[63]), by allowing consumers to move their data among competing entities, and thus enabling them to switch suppliers and/or multi-home (OECD, 2021[64]), data portability can reduce the risk of consumers becoming 'locked-in' to incumbent services. Moreover, data portability measures

[26] It provides that individuals "should have the right to obtain from a data controller, or otherwise, confirmation of whether the controller has data relating to them [and] to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them".

[27] Article 20, GDPR.

[28] Section 1798.100(d), California Consumer Privacy Act of 2018.

[29] Article 18, Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018.

[30] Bill C-27, currently before the House of Commons Standing Committee on Industry and Technology, includes amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) mainly through the proposed Consumer Privacy Protection Act (CPPA). In Québec, the right to portability comes into force on 22 September 2024 through Québec Act 25, amending the Québec Act respecting the protection of personal information in the private sector (Québec, 2023[92]).

can shift competition between suppliers away from the collection of data towards the analysis of data to gain insights, exploiting the non-rivalrous nature of data, thus potentially reducing one source of competitive advantage of large platforms.

However, by mandating data portability in order to strengthen competition, in specific situations users' data privacy risks being degraded. By decreasing the switching costs associated with data (i.e. it will be easier to access them later on), data portability may make users more willing to provide their data to a platform. As a result, users may exercise less scrutiny over the safeguards put in place by the recipient firm. Thus, data may be ported to companies with disparate size, security and risk management abilities, which can raise concerns for data security (Personal Data Protection Commission, Singapore, 2019[65]). Concerns have also been raised that, if portability applies horizontally, without regard to market power, in some circumstances the damage to smaller firms stemming from their (relatively scarce) data being ported to data-richer competitors might end up reinforcing the latter's dominance (Krämer, Senellart and De Streel, 2020[66]).

Providing for the right to data portability is not *per se* sufficient to give actual control and empowerment to data subjects: guidance materials, standards, codes of conduct as well as technological solutions such as open APIs are usually needed to improve the effective exercise of the right (Wong and Henderson, 2019[67]). Without the necessary infrastructure, individuals cannot make use of direct data portability between data holders (Kuebler-Wachendorff et al., 2021[68]). Sectoral initiatives may be more effective in implementing data portability, as observed with regard to open banking (OECD, 2023[69]) and open finance (OECD, 2023[70]). In conclusion, it is crucial to ensure high levels of data privacy in data portability arrangements, and the impact of the latter on both data privacy and competition would warrant further research.

A second example strictly linked to data portability is that of interoperability requirements, which have generally been considered to be more effective in restraining market power in digital markets than data portability in isolation. Interoperability refers to the ability of products and services at different levels (vertical interoperability) or at the same level (horizontal interoperability) of the digital value chain to work together (for more details see also (OECD, 2021[64]; 2023[63])). This is different to legal interoperability, which may be understood as "the ability of different privacy and data protection regimes, or legal frameworks, to work together at multiple levels through policy and practical arrangements and thereby bridge any differences in approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data" (Robinson, Kizawa and Ronchi, 2021[71]).

Measures preventing restrictions of interoperability or mandating interoperability between competitors' products or services aim at enhancing competition within individual ecosystems or between different ecosystems, depending on the type of interoperability (see also (OECD, 2023[63])). Under competition law, interoperability can be imposed as a remedy to a competition infringement, or mandated under *ex ante* digital regulations, in order to address barriers to entry, enable competitors' access, for instance to mobile ecosystems and app stores[31], and more broadly increase market contestability.

However, although interoperability can be imposed within the limits of data privacy laws, it can also be seen as harmful to data privacy "as continuous and real time access to data by competing services might entail a significant breach of privacy" (OECD, 2021[72]). Data privacy concerns are related to the fact that interoperability may potentially expose more personal data, and its implementation requires a careful interaction with the security settings of the entities involved to avoid an extension of the attack surface for criminal enterprises (Cyphers and Doctorow, 2021[73]).

[31] E.g. the Google JuicePass case investigated by the Italian competition authority (Decision No. 29645) or in the decision against Google by the French competition authority (Decision 21-D-11).

Furthermore, interoperability may potentially pose risks to data privacy: as the lack of interoperability *de facto* represents a safeguard for the data privacy principle of purpose limitation, removing this technical barrier (via the introduction of interoperability across systems) demands higher awareness of data protection and might require further safeguards (EDPS, 2023[74]). Data privacy safeguards to address this risk would tend to involve data subjects, to increase their control. In any case, interoperability needs to take place in a way that is respectful of data privacy. As it has been noted, data sharing between unconnected businesses must comply with the same data privacy principles, requirements and objectives as internal data sharing (CMA & ICO, 2021[75]).

Given the importance of data to effectively compete in digital markets dominated by platform ecosystems, measures contemplating a mandatory access to data held by such platforms can also be envisaged in specific situations, in particular to mitigate the risk of exclusionary practices. On the premise that data can constitute a barrier to entry and expansion, certain *ex ante* regulations foresee data access and data sharing obligations for selected platforms with "gatekeeper" power, consisting for instance in "granting access to a firm's dataset upon request of another (actual or potential competitor) firm" (OECD, 2021[72]).

Under competition law, access to data can generally be obtained only in exceptional circumstances, for example if data is considered an essential input and the essential facility doctrine can apply (Colangelo and Maggiolino, 2017[76]; OECD, 2020[42]). Remedies in antitrust cases, ordering dominant companies to share personal data with competitors, are not common. On the other hand, if imposed, such competition remedies might lead to data privacy questions.

Indeed, granting access to data can have implications for data privacy as, for example, data privacy law is concerned about possible breaches of personal data stemming from other parties' access. This potential underlying tension may give rise to divergences between enforcement of competition law and data privacy. This is especially the case if consent is required for the sharing of data, since obtaining consent from a vast number of users may prove costly or impracticable (Gal and Aviv, 2020[77]).

Some commentators have focused on consent and portrayed it as the only available lawful basis for processing personal data. This, in turn, has given rise to concerns that data privacy law may limit competition and lead to an increase of concentration in digital markets (Tombal, 2021[78]). However, this potential divergence has to be assessed on a case-by-case basis. For example, in the *GDF Suez* case, the French competition authority ordered the company to grant competitors access to information on its customers. However, after consultation with the data protection authority and following the latter's opinion, users were provided with a notice and the possibility to object (Autorité de la concurrence, 2014[79]). Indeed, authorities have noticed that companies may raise security concerns as a pretext for anticompetitive conduct and have expressed the intention to better scrutinise claims that restrictions on interoperability are needed to protect data privacy (FTC, 2023[80]), as explained below.

3.2. Data privacy defence

Despite being somewhat a standalone matter, it is worth addressing here the concerns around the so-called data privacy defence in abuse of dominance cases, in that it brings to light interesting aspects of the antitrust-privacy interplay. This novel phenomenon – which is expected to continue (Chen, 2023[4]) – sees the use of data privacy as a defence by dominant companies to refuse access to their dataset when this is necessary to compete (Ohlhausen, 2019[81]), or, alternatively, the use of an increased level of data privacy offered to end users as a justification for potentially anticompetitive conducts (Colangelo, 2023[2]; Douglas, 2021[1]).

This can also be linked to the use of double standards of data privacy by large data holders.[32] Relying on lower visibility on data circulating internally than on data shared with third parties, holders apply low personal data privacy standards to themselves within the ecosystem to gain a competitive advantage ("internal data free-for-all"), while applying stricter data privacy conditions to third parties for reusing their data. This can raise entry barriers and strengthen the platform's dominant position on the data markets (Tombal, 2021[78]), while being articulated as compliance with data privacy requirements.

In terms of possible enforcement action, in such situations it is important to differentiate between cases where the data privacy measure used as a shield is within the limits of what is mandated by data privacy law, and cases where it goes beyond that. Indeed, as mentioned at the beginning of this chapter, data privacy laws can in such instances provide a yardstick in the conduct's assessment. While in the former case it is for data protection authorities to ensure that the platform would achieve internally the mandated level of compliance that is also required of third parties, in the latter case the assessment of a conduct that can be detrimental to competition while being data privacy enhancing might be more complex and require substantial co-operation between authorities.

One relevant example is the French *Apple ATT* investigation[33], where the French competition authority solicited the observations of the French data protection authority (CNIL) on the questions related to personal data protection. In 2020 Apple implemented a feature called App Tracking Transparency (ATT), an opt-in mechanism for users to consent to being tracked for advertising purposes. However, this mechanism differentiated between third-party app developers and apps developed by Apple, allegedly facilitating discriminatory privacy policies to the advantage of Apple.

The French competition authority received a complaint that, under EU law, Apple's practice would constitute an abuse of dominance by imposing unfair trading conditions and a supplementary obligation. Considering in its assessment the opinion provided by the CNIL, the competition authority established that Apple's privacy-enhancing objective behind its ATT prompt would constitute a legitimate exercise of its commercial policy and not an anticompetitive conduct as such. Moreover, while being an additional protection measure with respect to GDPR, it could not be considered excessive nor disproportionate. Whilst rejecting the request for urgent interim measures, the authority has continued its investigation[34].

This initial decision was the result of the collaboration between the two regulators and seems to show that the conduct under investigation legitimately aimed at improving users' data privacy. However, the question of whether data privacy is the real motivation behind a practice and the risk that data privacy concerns could be used to hinder competition remains open (see also (Colangelo, 2023[2]; Giovannini, 2021[82]; Carugati, 2021[58])). The recent DoJ lawsuit against Apple[35] also mentions the risk of a "privacy shield", highlighting how "Apple wraps itself in a cloak of privacy, security, and consumer preferences to justify its anticompetitive conduct".

Similar concerns around the potential effects of privacy policies on digital advertising competition have also been addressed in the Google's Privacy Sandbox investigations, which saw collaboration between the competition authority (CMA) and the privacy regulator (ICO) in the UK (see also Box 4.1).

[32] This is related to the broader issue of digital platforms initially being 'open' and gradually silo-ing off their services once they reach maturity and the market tips under the rationale of privacy protection.

[33] https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021-04/21d07_en.pdf

[34] Differently from France's investigation, the ATT framework is under scrutiny in a number of other jurisdictions as a potential form of discriminatory self-preferencing.

[35] Case 2:24-cv-04055 https://www.justice.gov/opa/media/1344546/dl?inline

3.3. Compliance issues and overlapping investigations

In addition to the specific examples mentioned above, there are other aspects to consider when analysing the potential for tensions to emerge between competition and data protection authorities' perspectives, as this might require increased co-operation between the two authorities.

One such instance is the matter of overlapping investigations. As shown by the *Meta Platforms* case, certain conducts in digital markets could potentially raise issues under both competition and data privacy laws, e.g. infringements of data privacy rules that also qualify as abuse of dominance infringements. This could lead to the risk that both laws could be enforced against the same behaviour. If this happens, a possible concern, in theory, could be that parallel investigations and sanctions could be in violation of the *ne bis in idem* principle (Evrard et al., 2023[83]; Stauber, 2019[34]).

However, the protection against double jeopardy is subject to specific conditions, one being that the legal interest protected by the respective rules needs to be the same (Harrison, Zdzieborska and Wise, 2022[84]). Advocate General Bobek's Opinion in *bpost*[36] made further clarifications on this point that may be relevant for the interplay antitrust-privacy laws, in that the two laws protect different legal interests.

In particular, the Opinion determined that the *ne bis in idem* principle does not prevent competition law enforcement and sanctioning against a company that was already prosecuted for failing to comply with sectoral regulations, "provided that, in general, the subsequent set of proceedings are different either as to the identity of the offender, or as to the relevant facts, or as to the protected legal interest the safeguarding of which the respective legislative instruments at issue in the respective proceedings pursue"[37]. As competition and data privacy legislations protect different legal interests (albeit in a complementary manner), the *ne bis in idem* principle would seem not to be violated.

Parallel investigations can also result in inconsistent approaches by competition and data protection authorities, especially in circumstances where questions around interoperability or access to data are at stake. Although this risk is inherent to enforcement in digital markets, where antitrust, data privacy and also consumer protection issues are often intertwined, frameworks for co-operation between authorities can help reduce frictions and divergences. Chapter 4below will explore the matter of co-operation in more detail.

Finally, some commentators have observed that compliance with data privacy laws can raise barriers to entry for smaller businesses, or more generally create advantages for the incumbents. Although this can apply also in other areas, as regulatory compliance costs are often relatively higher for small and medium enterprises (SMEs), the compliance efforts required by the growing number of data privacy laws globally may affect competition in certain markets.

As highlighted in (OECD, 2020[42]), this raises the question of whether the objectives of the relevant data privacy legislation can be achieved in a way that minimises (negative) impacts on competition. In line with this, the 2023 joint declaration by the French competition authority and the CNIL[38] note how, in light of the interplay between the two legal frameworks and the existing evidence that data privacy is proportionally less onerous for the largest players in the market, "the impact of privacy protection standards on the functioning of competition shall be taken into account at the stage when these standards are developed, just as the objective of protecting privacy can be taken into account as part of the competitive analysis" (Autorité de la concurrence; Commission nationale de l'informatique et des libertés, 2023[85]).

[36] Case C-117/20

[37] Advocate General Bobek proposes a unified test for the protection against double jeopardy (ne bis in idem) under the EU Charter of Fundamental Rights (europa.eu)

[38] https://www.cnil.fr/sites/cnil/files/2023-12/competition_and_personal_data_a_common_ambition_joint_declaration_by_the_cnil_and_the_adlc.pdf

4 Co-operation between authorities

The previous chapters highlighted the growing need for co-operation between competition and data protection authorities. There appears to be consensus that where data is a key parameter of competition, companies' collection, manipulation, and use (or misuse) of users' data can have relevant implications for both data protection and competition authorities. The risk of divergences between the two regulatory communities should thus be minimised.

The necessity for co-operation is also amplified as more regulatory frameworks applicable to data-driven markets are implemented, or are in the process of being adopted, at both the national and the supra-national levels. As highlighted in the joint declaration by the CNIL and French competition authority, "this very rich regulatory data landscape will necessarily lead to new interactions" (Autorité de la concurrence; Commission nationale de l'informatique et des libertés, 2023[85]), and how such interactions will be governed will have a role in how effectively the practices of platforms and more generally digital companies can be addressed.

While the need for co-operation is now well-established, the most effective means to do so and the practical implications of such co-operation are still being explored. Jurisdictions worldwide showcase a range of models for co-operation, each offering interesting insights and lessons.

Several instances indicate that *ad hoc* co-operation on specific investigations concerning both competition and data privacy is already taking place, at least at an incipient stage and in certain jurisdictions. This has been the case in the German *Meta Platforms* case mentioned above and the *Google Privacy Sandbox* case in the UK (see Box 4.1 below). Similarly, co-operation between the CNIL and the French competition authority started as far back as 2014 in the context of the *GDF Suez* case, as discussed above.

The principle of "sincere co-operation" enshrined in Article 4(3) TEU, which resurfaced in the preliminary ruling of the Court of Justice of the EU in the *Meta Platforms* case (as discussed above), opens the door to stronger co-operation between competition and data protection authorities, and potentially a more integrated approach in those cases where data collection is at the core of the relevant companies' business models. The need for co-operation has also recently emerged in Canada, where – in the context of the competition law reform – the data protection authority has recommended a legislative authorisation for the two authorities to "collaborate on investigations, inquiries or other formal compliance matters" (Office of the Privacy Commissioner of Canada, 2023[86]).

However, how such co-operation should be structured and on which aspects it should focus is to be determined very carefully. Informal co-operation may often take place without legislative reforms or a formal legal basis. For more advanced co-operation, a relevant legal basis would be needed for information sharing between authorities and possibly for other kinds of co-ordinated action.

Legislation may also provide one regulator with a secondary duty related to the other's policy area: for example, in the UK, with the Data Protection and Data Information Bill (a reform of the Data Protection Act 2018), there will be a specific secondary duty for the data protection authority in relation to competition and to economic growth (in addition to the obligation under the Deregulation Act 2015 for regulators to have regard to the desirability of promoting economic growth) (UK Parliament, 2023[51]).

Co-operation would be especially beneficial for newer matters such as those related to the interplay between data privacy and competition. In particular, co-operation in this area would be central to achieve

a better understanding of business models and market dynamics, where data is a key parameter of competition or companies are competing on data privacy itself.

Moreover, in more complex cases around platform ecosystems, dialogue between regulators would allow for an optimal use of competition and data privacy laws so that the goals of one can be maximised while minimising the risks of undermining the other. For instance, an appropriate approach may be to determine in advance which points of the ecosystems should be opened to competition as a priority, and which ones may imply too high a risk for data privacy. For many issues, only continuous engagement and dialogue among regulators over time will allow them to identify the most mutually beneficial manner of implementing both policy areas.

Box 4.1. Co-operation in the UK Google Privacy Sandbox

In January 2021, the Competition and Markets Authority (CMA) opened an investigation into Google's proposals to remove third-party cookies and other functionalities from its Chrome browser and replace them with new Privacy Sandbox tools for targeted advertising. This followed concerns that Google's proposals, which had the stated objective of enhancing data privacy on the web through a set of open standards, could amount to an abuse of dominant position.

Working with the Information Commissioner's Office (ICO), in February 2022 the CMA accepted legally binding commitments by Google, which were designed to ensure users' data privacy would be improved without hampering competition.

These include obligations around transparency and the authorities' involvement in the Privacy Sandbox testing process, a standstill period before the removal of third-party cookies, allowing the CMA to solve all remaining competition law concerns, as well as commitments around Google's use of users' personal data and tracking. Moreover, Google commits to ensure that the design, development, and implementation of the Privacy Sandbox will not distort competition by discriminating against rivals in favour of Google's advertising products and services (see also Competition and Markets Authority, 2022).

It is worth noting that, pursuant to the Commitments, the CMA consults the ICO on possible remaining concerns on data privacy impacts. The latest report on the implementation of the Commitments acknowledges the possibility that changes made by Google for personal data protection purposes may have negative implications for ad tech firms, advertisers and publishers as well as "the need for careful consideration of these issues so that competition and data protection objectives are promoted overall to the benefit of consumers" and provides information on the ICO's engagement (Competition and Markets Authority, 2024).

Sources:

Competition and Markets Authority (2022), Case 50972 - Privacy Sandbox - Google Commitments Offer, https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf.

Competition and Markets Authority (2024), CMA Q4 2023 update report on implementation of the Privacy Sandbox commitments, https://assets.publishing.service.gov.uk/media/65ba2a504ec51d000dc9f1f5/CMA_Q4_2023_update_report_on_implementation_of_the_Privacy_Sandbox_commitments_PDFA_1.pdf.

Secondly, certain agencies have both data protection and competition powers. For instance, in addition to being one of two federal agencies that enforce US antitrust laws, the Federal Trade Commission (FTC) is also responsible for the enforcement of consumer protection and privacy laws in the US. One example of how parallel supervision could take place is the Facebook/Whatsapp merger, cleared by the FTC in 2014.

In light of the transaction, the FTC's Bureau of Consumer Protection[39] notified the parties about their pre-existing obligations to protect their user's data privacy, thus complementing the FTC's Bureau of Competition's intervention by acknowledging the key role of data privacy both for users' rights and as a competition parameter that could have been hampered by the transaction. Recently, the FTC has highlighted the importance of integrating competition concerns into its data privacy work, to ensure complementarity between its two missions and to look "with both privacy and competition lenses at problems that arise in digital markets" (FTC, 2021[60]).

Similarly, in Colombia, the Superintendence of Industry and Commerce (SIC) is responsible for both competition and data privacy, amongst other duties such as consumer protection and industrial property rights. This centralisation of powers and expertise within the same agency may allow for a better understanding of data-related dynamics in digital markets, as well as a more effective inclusion of different policy considerations in enforcement cases, reducing the need for external coordination and the risk of divergences.

For instance, in the context of the proposed merger between Bancolombia, Banco Davivienda, and Banco de Bogotá, in 2019 the SIC provided an opinion[40] to the financial markets' regulator (Superintendencia Financiera de Colombia), responsible for reviewing the transaction. In light of its double competence as antitrust and data privacy regulator, in its opinion the SIC provided a number of recommendations around the use of data, in order to address the potential harm to competition. These involved processing the personal data of the merged entity's customers in compliance with data privacy laws, as well as obligations around data portability and interoperability, including a prohibition to automatically transfer the parties' customers' data to the merged entity without explicit and informed prior authorisation.

The need to address the new enforcement challenges posed by digital markets has also led to the creation of new fora for exchange and co-operation. Examples include the Digital Regulation Co-operation Forum (DRCF) created in 2020 in the UK, the Digital Regulation Co-operation Platform (SDT) launched in the Netherlands in 2021[41], the Digital Platform Regulators Forum (DP-REG) launched in Australia in 2022[42], and the Irish Digital Regulators Group also launched in 2022 (CCPC, 2023[87]). These fora are by and large voluntary in nature and aim to deliver coherent approaches to regulation in the digital sphere. They have recently launched an International Network for Digital Regulation Co-operation (INDRC) to foster discussion between regulators on matters of coherence across digital regimes (DRCF, 2023[88])).

The *Pôle d'expertise de la regulation numérique* (PEReN)[43] established in 2020 in France pursues a similar objective through a different structure: it is an inter-ministerial service expertise hub on data science, for the benefit of government services and independent authorities (including competition and data protection authorities). Through these different initiatives, public authorities can improve their expertise on regulatory challenges in the digital environment, share best practices, and strengthen their ability to address issues such as those at the intersection of competition and data privacy law.

A similar initiative had been proposed by the European Data Protection Supervisor. In consideration of the impact of big data, machine learning and artificial intelligence, the EDPS proposed the establishment of a Digital Clearinghouse for privacy, competition and consumer protection agencies to share information and

[39] See also FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition | Federal Trade Commission.

[40] BANCOLOMBIA - DAVIVIENDA - BANCO DE BOGOTÁ.pdf (sic.gov.co)

[41] https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt

[42] https://dp-reg.gov.au/

[43] https://www.peren.gouv.fr/qui-sommes-nous/

discuss enforcement in the interests of the individual, and has organised several meetings and published statements (EDPS, 2020[89]).

Moreover, in the EU the EC has recently established a High-Level Group on the DMA, composed of 30 representatives nominated from a number of authorities, namely the Body of the European Regulators for Electronic Communications (BEREC), the European Data Protection Supervisor (EDPS) and European Data Protection Board, the European Competition Network (ECN), the Consumer Protection Co-operation Network (CPC Network), and the European Regulatory Group of Audiovisual Media Regulators (ERGA).

The general objective of these co-operation fora is to bring together different types of regulators whose activities and expertise have a key role to play for regulation and enforcement in digital markets, allowing them to work together in a more effective and agile way, providing a coherent approach to common issues, exchanging viewpoints from the respective fields to achieve better outcomes. These can also provide a model of *ad hoc* co-operation for specific industries in other jurisdictions, where markets, such as digital ones, could require joint interventions on a regular basis.

At the OECD, several work streams have highlighted the importance of co-operation among regulators to address challenges related to digital markets. For example, with regard to open banking, the complexity and overlaps between the mandates of different regulators have been acknowledged and have underlined the need for effective co-operation among regulators as "a prerequisite for co-ordinated enforcement" (OECD, 2023[69]).

In particular, data protection authorities have expressed the need for, and an interest in, stronger co-operation with other public regulators, such as competition authorities. In the context of the review of the 2007 Recommendation on cross-border enforcement of privacy laws[44], the issue of cross-sectoral and cross-domain co-operation has been identified as requiring specific consideration.

In conclusion, there seems to be an emerging consensus in different countries on the need to act to facilitate co-operation between regulators. This can take a host of different forms and may be based on informal activities of the regulators themselves or legislative reforms by policy makers. Whilst the complexity of the effort is considerable, the potential benefits in terms of effective achievement of policy objectives would be major.

https://www.oecd.org/digital/review-of-the-oecd-recommendation-on-cross-border-co-operation-in-the-enforcement-of-laws-protecting-privacy-67774f69-en.htm.

5 Conclusion

The growing significance of data, particularly of personal data, for companies' business strategies underscores the intertwined nature of safeguarding competitive markets and protecting individual data privacy. This calls for a holistic vision at the highest levels of policymaking and coordinated action by competition and data protection authorities.

In theory, more competitive markets could promote enhanced data privacy as a competitive attribute, and stricter regulatory oversight on companies' personal data collection and processing practices could help to prevent the entrenchment of market power. In reality, these conceptual synergies do not always materialise in practice, including due to a legacy of siloed approaches to regulation.

Technological advancements, digital market developments and the rise of large platform ecosystems have introduced new complexities and enforcement challenges that can be difficult to manage for either competition or data protection authorities. Nevertheless, the current landscape of highly concentrated digital markets with established business models reliant on vast amounts of personal data collected over the years, underscores the need to transcend traditional conceptual and legislative frameworks to achieve more integrated enforcement strategies.

As discussed in Chapter 3, several issues have already emerged, becoming the object of investigation or enforcement action by competition and/or data protection authorities in a number of cases. For example, the sharing of data across different companies may enhance competition, but needs to uphold high level of personal data protection. Furthermore, the emergence of *ex ante* data portability or interoperability obligations in more recent legislative frameworks makes the intersection of competition and data privacy law ever more complex and crucial for the digital economy.

Chapter 4 has illustrated emerging models of co-operation aimed at harnessing synergies across different regulatory bodies. Yet, these co-operative efforts might, at times, face obstacles such as misaligned priorities and differing enforcement preferences and solutions. Moreover, questions arise regarding whether competition agencies should actively pursue antitrust remedies that are the most data privacy enhancing, or whether data protection should prioritise data privacy measures that promote competition. Addressing these questions will require sincere and continuous co-operation, including alignment on the conceptual framework and priority outcomes that underlie such co-operation.

In the long term, effective cross-regulatory co-operation is paramount. Regulators should strive to establish a mutual understanding of their respective priorities and ways of working, sharing expertise and resources, to better appraise the functioning of new business models and what each community or (ideally, both) should focus on addressing to achieve common goals in digital markets.

The OECD can offer support to both policy communities by providing a platform to exchange expertise and lay the groundwork for constructive and sustainable strategies to effectively address the policy and regulatory challenges associated with digital markets, within and across jurisdictions.

References

ACM (n.d.), *The Digital Regulation Cooperation Platform (SDT)*, https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt. [98]

Acquisti, A., T. Curtis and W. Liad (2016), "The Economics of Privacy", *Journal of Economic Literature*, https://doi.org/10.1257/jel.54.2.442. [13]

Akman, P. et al. (2022), *International Perspectives on Privacy and Competition Law*, American Bar Association, https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-february/international-perspectives-on-privacy-and-competition-law/. [30]

Autorità Garante della Concorrenza e del Mercato (2021), *PS11147-PS11150 - Sanzioni per 20 milioni a Google e ad Apple per uso dei dati degli utenti a fini commerciali*, https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150. [95]

Autorité de la concurrence (2014), *Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité*, https://www.autoritedelaconcurrence.fr/sites/default/files/commitments/14mc02.pdf. [79]

Autorité de la concurrence; Bundeskartellamt (2016), *Competition Law and Data*, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2. [31]

Autorité de la concurrence; Commission nationale de l'informatique et des libertés (2023), *Competition and personal data: a common ambition*, https://www.cnil.fr/sites/cnil/files/2023-12/competition_and_personal_data_a_common_ambition_joint_declaration_by_the_cnil_and_the_adlc.pdf. [85]

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", *Antitrust Bulletin*, pp. 428-446, https://deliverypdf.ssrn.com/delivery.php?ID=365086110124001106028081013073124029031084070081044092070068077070127099105088071113057037031013031061114092094022087108075073015055013006080117012006091102117099095024042036092117121119001064085101065005005001. [6]

Bundeskartellamt (2019), *Background information on the Bundeskartellamt's Facebook proceeding*, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6. [26]

Carugati, C. (2021), "The Antitrust Privacy Dilemma", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968829. [58]

CCPC (2023), *Annual Report 2022*, https://www.ccpc.ie/business/wp-content/uploads/sites/3/2023/08/2023.06.29_CCPC_Annual-Report-2022.pdf. [87]

Chen, S. (2023), “The Latest Interface: Using Data Privacy as a Sword and Shield in Antitrust Litigation”, *Hastings Law Journal*, Vol. 74/2, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=4017&context=hastings_law_journal. [4]

CMA (2016), *Retail banking market investigation*, https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-order. [93]

CMA & ICO (2021), *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, https://assets.publishing.service.gov.uk/media/60a3c893d3bf7f288aaa5c9b/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf. [75]

CNIL (2024), *The economic impact of GDPR, 5 years on*, https://www.cnil.fr/en/economic-impact-gdpr-5-years?mkt_tok=MTM4LUVaTS0wNDIAAAGSSYvBUnQ69vKyyCn2VljmS0b9HmoVKdxrkC4TBOY7EemoRpCPb8evKXehZ9UP0PaRjEYG12Fb-rEp1WOTwmvC1IE6KixEJzr8nkH1fKnKDVPeTA. [50]

CNIL (2023), *Data economy: CNIL strengthens its analysis skills and publishes its work programme*, https://www.cnil.fr/en/data-economy-cnil-strengthens-its-analysis-skills-and-publishes-its-work-programme. [55]

CNIL (2021), *Scènes de la vie numérique*, Cahiers IP No. 8, https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_cahier_ip8.pdf. [19]

Colangelo, G. (2023), “The Privacy/Antitrust Curse: Insights From GDPR Application in Competition Law Proceedings”, *ICLE White Paper*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4599974. [2]

Colangelo, G. and M. Maggiolino (2017), “Big Data as a Misleading Facility”, *European Competition Journal*, Vol. 13/2-3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2978465. [76]

Competition and Markets Authority (2024), *CMA Q4 2023 update report on implementation of the Privacy Sandbox commitments*, https://assets.publishing.service.gov.uk/media/65ba2a504ec51d000dc9f1f5/CMA_Q4_2023_update_report_on_implementation_of_the_Privacy_Sandbox_commitments_PDFA_1.pdf. [94]

Competition and Markets Authority (2023), *AI Foundation Models Initial Report*, https://assets.publishing.service.gov.uk/media/650449e86771b90014fdab4c/Full_Non-Confidential_Report_PDFA.pdf. [61]

Competition and Markets Authority (2022), *Case 50972 - Privacy Sandbox - Google Commitments Offer*, https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf. [91]

Condorelli, D. and J. Padilla (2023), “Data-Driven Envelopment with Privacy-Policy Tying”, *The Economic Journal*, Vol. 134, https://watermark.silverchair.com/uead090.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA1wwggNYBgkqhkiG9w0BBwagggNJMIIDRQIBADCCAz4GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMKu4KlIRq7KwTNxUAAgEQgIIDD2_5IpUV4lMl8NRSPELdJKe1ojqmAIkSNtanz5VdGf1AX5o. [41]

Condorelli, D. and J. Padilla (2020), "Harnessing Platform Envelopment In the Digital World", *Journal of Competition Law & Economics*, Vol. 16/2, https://watermark.silverchair.com/nhaa006.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA1swggNXBgkqhkiG9w0BBwagggNIMIIDRAIBADCCAz0GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMl3xSBxaJ1-eLoJSYAgEQgIIDDin-UGzHWvTIEqaYCiZYny9D-1jqcjNz_P1XVW3js8HDamy. [40]

Costa-Cabral, F. and O. Lynskey (2017), "Family ties: the intersection between data protection and competition in EU law", *Common Market Law Review*, Vol. 54/1, pp. 11-50, https://core.ac.uk/download/pdf/77615074.pdf. [7]

Court of Justice of the European Union (2023), *Meta Platforms and others v Bunderskartellamt*, https://curia.europa.eu/juris/document/document.jsf?docid=275125&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=2106784. [44]

Cyphers, B. and C. Doctorow (2021), *Privacy Without Monopoly: Data Protection and Interoperability*, https://www.eff.org/wp/interoperability-and-privacy#Risksandmitigations. [73]

D'Amico, A. (2023), "Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?", *Utrecht University School of Law Research Paper*, https://ssrn.com/abstract=4492347. [49]

Datatilsynet (2024), *Request for an EDPB opinion on "consent or pay"*, https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/. [52]

Douglas, E. (2022), "Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis", *Notre Dame L. Rev. Reflection*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167390. [3]

Douglas, E. (2021), "Digital Crossroads: The Intersection of Competition Law and Data Privacy", *Temple University Legal Studies Research Paper*, Vol. 40, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737. [1]

Douglas, E. (2021), "The New Antitrust/Data Privacy Law Interface", *The yale Law Journal*, Vol. 130, https://www.yalelawjournal.org/forum/the-new-antitrustdata-privacy-law-interface. [33]

DP-REG (2023), *Digital Platform Regulators Forum*, https://dp-reg.gov.au/. [99]

DRCF (2023), *Launch of the International Network for Digital Regulation Cooperation (INDRC)*, https://www.drcf.org.uk/news-and-events/news/launch-of-the-international-network-for-digital-regulation-cooperation-indrc. [88]

EDPB (2024), *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf. [27]

EDPB (2023), *EDPB Launches Data Protection Guide for small business*, https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business_en. [96]

EDPB (2023), *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf. [46]

EDPS (2023), *Opinion 1/2023 on the Proposal for an Interoperable Europe Act*, https://www.edps.europa.eu/system/files/2023-01/2022-1196_d0089_opinion_en.pdf. [74]

EDPS (2020), *Big Data & Digital Clearinghouse*, https://www.edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en. [89]

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*, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf. [45]

Eisenmann, T., G. Parker and M. Van Alstyne (2011), "Platform Envelopment", *Strategic Management Journal*, Vol. 32/12, https://www.jstor.org/stable/pdf/41261793.pdf?refreqid=fastly-default%3A2354ff09656bb981655de5258f31bb56&ab_segments=&origin=&initiator=&acceptTC=1. [90]

Evrard, S. et al. (2023), *Intersection of competition law and data privacy poses challenges to market regulation*, Global Competition Review, https://www.lexology.com/library/detail.aspx?g=6f6c5c63-2ae3-4e81-a4f0-2cb3587787d8. [83]

Fara, D. and J. Moss (2023), *Revisiting EDPB, ICO approaches to administrative fines*, https://iapp.org/news/a/revisiting-edpb-ico-approaches-to-administrative-fines/?mkt_tok=MTM4LUVaTS0wNDIAAAGQHRP9ZpxDZoYNrZUgLu5JGdp0C3YF2r1Lne9t9rM_t7DqfVnNtLzr1fS45c5cccQuhhJyhXosM3CfH4pRhSB9cB3nN-6Obmc1MXR-4SarcXTnOQ. [48]

FTC (2023), *Interoperability, Privacy, & Security*, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security#ftn6. [80]

FTC (2021), *FTC Report to Congress on Privacy and Security*, https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf. [60]

Gal, M. and O. Aviv (2020), *The Competitive Effects of the GDPR*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444. [77]

Garante (2019), *Big Data. Linee guida e raccomandazioni di policy. Indagine conoscitiva congiunta di Agcom, Agcm e Garante privacy*, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9122609. [56]

Giovannini, V. (2021), *the french Apple competition & privacy case*, https://competition-forum.com/the-french-apple-competition-privacy-case/. [82]

Górecka, A. (2022), *Competition Law And Privacy: An Opinion on The Future of a Complicated Relationship*, https://competitionlawblog.kluwercompetitionlaw.com/2022/06/08/competition-law-and-privacy-an-opinion-on-the-future-of-a-complicated-relationship/. [32]

Graef, I., D. Clifford and P. Valcke (2018), "Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law", *International Data Privacy Law*, Vol. 8, pp. 200-223, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216198. [43]

Harrison, P., M. Zdzieborska and B. Wise (2022), *Ne Bis in Idem: The Final Word?*, https://competitionlawblog.kluwercompetitionlaw.com/2022/04/07/ne-bis-in-idem-the-final-word/. [84]

ICO (2024), *Data Protection Fining Guidance*, https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/. [47]

ICO (2023), *The ICO's Impact Assessment Framework*, https://ico.org.uk/media/about-the-ico/documents/4027020/ico-impact-assessment-framework.pdf. [57]

Irish Data Protection Commission (2022), *In the matter of LB, a complainant, concerning a complaint directed against Meta Platforms Ireland*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29.pdf. [23]

Irish Data Protection Commission (2022), *In the matter of TSA, a complainant, concerning a complaint directed against Meta Platforms Ireland*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf. [24]

Kemp, K. (2020), "Concealed data practices and competition law: why privacy matters", *European Competition Journal*, https://doi.org/10.1080/17441056.2020.1839228. [37]

Krämer, J., P. Senellart and A. De Streel (2020), *Making data portability more effective for the digital economy: economic implications and regulatory challenges*, https://pure.unamur.be/ws/portalfiles/portal/54626944/8588.pdf. [66]

Kuebler-Wachendorff, S. et al. (2021), "The Right to Data Portability: conception, status quo, and future directions", *Informatik Spektrum*, https://doi.org/10.1007/s00287-021-01372-w. [68]

Lande, R. (2008), "The Microsoft-Yahoo Merger: Yes, privacy is an Antitrust Concern", *University of Baltimore Legal Studies Research Paper*, Vol. 06/714, https://deliverypdf.ssrn.com/delivery.php?ID=107064121121026003087085015003102002098014089077064041076070095098122003091114116094058057003006039016043114012117112084107104106078031069085009083097107065119096047093042123015122081089100079004021103071092110. [28]

MacLachlan, M. (2024), *Class action liability following a data breach*, https://www.shoosmiths.com/insights/articles/class-action-liability-following-a-data-breach. [59]

OECD (2024), *Shaping a rights-oriented digital transformation*, https://one.oecd.org/official-document/DSTI/CDEP(2023)11/REV2/en. [18]

OECD (2023), *Data portability in open banking: Privacy and other cross-cutting issues*, https://doi.org/10.1787/6c872949-en. [69]

OECD (2023), *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, https://doi.org/10.1787/bf121be4-en. [53]

OECD (2023), "Explanatory memoranda of the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 360, OECD Publishing, Paris, https://doi.org/10.1787/ea4e9759-en. [20]

OECD (2023), *G7 inventory of new rules for digital markets: Analytical note*. [63]

OECD (2023), *Open finance policy considerations*, https://doi.org/10.1787/19ef3608-en. [70]

OECD (2023), *The Consumer Welfare Standard - Advantages and Disadvantages Compared to Alternative Standards*. [10]

OECD (2023), *Theories of harm for digital mergers*, https://www.oecd.org/daf/competition/theories-of-harm-for-digital-mergers-2023.pdf. [35]

OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en. [100]

OECD (2021), *Data portability, interoperability and digital platform competition*. [64]

OECD (2021), *Ex ante regulation and competition in digital markets*. [72]

OECD (2021), *Mapping Data Portability Initiatives, Opportunities and Challenges*, https://www.oecd.org/publications/mapping-data-portability-initiatives-opportunities-and-challenges-a6edfab2-en.htm. [62]

OECD (2020), *Competition in digital advertising markets*, https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets.htm. [25]

OECD (2020), *Consumer Data Rights and Competition*. [42]

OECD (2018), *Quality Considerations in Digital Zero-Price Markets*. [11]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [21]

OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris, https://doi.org/10.1787/5kgf09z90c31-en. [22]

OECD (2003), *The objectives of competition law and policy*. [9]

Office of the Privacy Commissioner of Canada (2023), *Submission of the Office of the Privacy Commissioner of Canada on the Competition Act reform*, https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_competion_230320/#fn33-rf. [86]

Ohlhausen, M. (2019), "Privacy and Competition: Friends, Foes, or Frenemies", *CPI Antitrust Chronicle* February, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/CPI-Ohlhausen.pdf. [81]

Ohlhausen, M. and A. Okuliar (2015), "Competition, Consumer Protection, and the Right Approach to Privacy", *Antitrust Law Journal*, Vol. 80/1, pp. 121-156, https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf. [29]

Pal, P. and H. Kumar (2021), "Data Sharing between WhatsApp and Facebook: The CCI Opens an Investigation Against the Social Juggernauts", *CPI Columns* June, https://www.competitionpolicyinternational.com/wp-content/uploads/2021/06/South-Asia-Column-June-2021-2-Full.pdf. [36]

PEReN (2021), *Qui sommes-nous ?*, https://www.peren.gouv.fr/qui-sommes-nous/. [97]

Personal Data Protection Commission, Singapore (2019), *Discussion paper on Data Portability*, https://www.cccs.gov.sg/-/media/custom/ccs/files/media-and-publications/publications/occasional-paper/pdpc-cccs-data-portability-discussion-paper---250219.ashx. [65]

Québec (2023), *Droit à la portabilité*, https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/acces-aux-renseignements-personnels/titre-par-defaut. [92]

Ranieris, E. (2021), *Why PETs (privacy-enhancing technologies) may not always be our friends*, https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/. [54]

Robertson, V. (2020), "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Law Market Review*, pp. 161-189, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3408971. [38]

Robinson, L., K. Kizawa and E. Ronchi (2021), *Interoperability of privacy and data protection frameworks*, http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf. [71]

Solove, D. (2006), "A Taxonomy of Privacy", *U. Pa. L. Rev.*, https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1. [12]

Stauber, P. (2019), *Facebook's Abuse Investigation in Germany and Some Thoughts on Cooperation Between Antitrust and Data Protection Authorities*, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/CPI-Stauber.pdf. [34]

Stucke, M. (2018), "Should We Be Concerned About Data-opolies?", *Georgetown Law Technology Review*, https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Stucke-pp-275-324.pdf. [39]

Tombal, T. (2021), "Data Protection and Competition Law: Friends or Foes regarding Data Sharing?", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826325. [78]

UK (2015), *Consumer Rights Act 2015*, https://www.legislation.gov.uk/ukpga/2015/15/contents/enacted. [8]

UK Parliament (2023), *Data Protection and Digital Information Bill*, https://bills.parliament.uk/bills/3430/publications. [51]

UN General Assembly (1966), *International Covenant of Civil and Political Rights*, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. [17]

UN General Assembly (1948), *Universal Declaration of Human Rights*, https://www.un.org/en/about-us/universal-declaration-of-human-rights. [16]

Waxman, O. (2018), "The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History", *Time*, https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/. [14]

Whitman, J. (2004), *The Two Western Cultures of Privacy: Dignity v. Liberty*, The Yale Law Journal, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/5038/The_Two_Western_Cultures_of_Privacy___Dignity_versus_Liberty.pdf?sequence=2&isAllowed=y. [15]

Wiedemann, K. (2023), "Can Data Protection Friendly Conduct Constitute an Abuse of Dominance under Art. 102 TFEU?", *Research Handbook on Competition Law and Data Privacy*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4520608. [5]

Wong, J. and T. Henderson (2019), "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz008. [67]