Wolfgang Kerber / Louisa Specht-Riemenschneider

SYNERGIES BETWEEN DATA PROTECTION LAW AND COMPETITION LAW

30. September 2021

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Verbraucherzentrale Bundesverband e.V.

Team Digital and Media

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

Contents

Figures and Tables

Executive Summary

I. Large digital firms and the problems for competition and data protection

1) **The huge economic power of the large digital (tech) firms** (in particular, Google, Facebook, Amazon, and Apple) has led to new and large threats to both competition on many markets and the privacy and data protection of all citizens. This is a big challenge for competition policy and data protection law.

2) In competition policy a broad opinion acknowledges that we have a **very large competition problem that cannot sufficiently be solved by traditional competition law**. This has led to the current far-reaching new policy initiatives, especially the "Digital Markets Act" proposal of the EU Commission with an ex-ante regulation of the behavior of gatekeepers.

3) These large digital firms collect a massive amount of **personal data** from consumers, who are not capable of making sufficiently voluntary and informed decisions about the collection and use of “their” personal data (information and behavioral market failure), which **endangers their informational self-determination and privacy**. This is a (so far publicly less discussed) huge challenge for data protection law.

II. Framework for analyzing the intertwinement of competition and data protection law

4) Due to the key role of personal data on many digital markets and the business models of these large digital firms, **both problems (competition and privacy/data protection) and both market failures (market power and information/behavioral problems) are deeply intertwined with each othe**r. This leads to a new and increasingly complex relationship between competition law and data protection law, and the need for an integrated analysis of competition and data protection problems with respect to the large digital firms.

5) For the analysis of this new relationship this report uses an **analytical framework**, which includes the two market failures "market power" and "information and behavioral problems" and the two policies "competition law" and "data protection law" for enabling a better analysis of the interaction effects between these two market failures and two policy regimes on digital markets. This economic policy approach allows for a better "mapping" of the problems, e.g. also with respect to conflicts and synergies of both policies.

6) Current discussions about competition and data protection have already shown the existence of **manifold interaction effects between both policy regimes**: Market power can have negative effects on privacy, information problems might impede competition, but there might

also be positive and negative effects of data protection law on competition, as well as of competition law on data protection. These **interaction effects can lead to conflicts but also offer the chance of synergies**, i.e. that competition law and data protection law can help each other for achieving better the objectives of both policies, namely competition and data protection.

7) The relationship between competition policy and data protection law is not only complementary. but due to the simultaneous existence of both market failures and the various interaction effects a **more integrative and collaborative approach between competition law, data protection law**, and also consumer law is necessary.

III. Some synergies and conflicts between data protection and competition law

8) The identification of synergies and conflicts between competition law and data protection law and how to deal with them is itself a complex problem. This is shown, in the following, by the analysis of a selected number of potential conflicts and synergies that have emerged in the current discussions.

9) **Competition and privacy**:

a) The main reason why so far competition did not work well with respect to leading to more **privacy-friendly data-collection practices of firms** is the unsolved market failure "information and behavioral problems". It also includes **"dark pattern" practices** of firms leading to informational and behavioral manipulation of consumers regarding their "consent".

b) It is unclear whether this market failure problem can be sufficiently solved by more information requirements as part of **"notice and consent" solutions**, or whether more far-reaching solutions are necessary. One particularly difficult additional problem arises from "data externalities".

10) **EU data protection law and competition**:

a) In the last years a discussion emerged that a strict data protection law (as the GDPR) with an **opt-in consent for collecting personal data might have negative effects on competition**, and might even favor, in particular, the large digital firms, because they might get easier consent than other (smaller) firms. Our critical analysis of this thesis leads to the following much more differentiated results:

b) The thesis that **larger and more diversified firms might have advantages** regarding costs of compliance with the GDPR compared to smaller firms might be – also partly confirmed by empirical studies – correct but this is true also for most other regulations and not specific for the GDPR.

c) The large digital firms can presumably often get easier "consent" for the collection and use of personal data. However, the **main reasons for this competitive advantage** are (aa) the **market power of the large digital firms**, which force the consumers to consent (due to a lack of choice), and (bb) the well-known **problem of underenforcement of the GDPR**, especially with respect to the large digital firms. This underenforcement problem of the GDPR is caused by a weak enforcement regime and a too high level of legal uncertainty.

d) If the GDPR was properly enforced and the market power problem solved, it can be expected that most of these competitive advantages of the large digital firms would be eliminated.

e) Therefore, the alleged conflict between a high level of data protection and competition only exists due to other unsolved problems. The correct policy conclusions are, hence, to solve the enforcement problems of the GDPR and deal effectively with the economic power of the large digital firms instead of weakening the standards of data protection law. This does not exclude the possibility to also find better solutions in data protection law that have positive effects on competition without endangering the objectives of data protection law.

11) Although the **data portability right of Art. 20 GDPR** is widely seen as potentially facilitating competition, the expected synergy effects could not be realized so far. The current efforts to make this data portability right more effective, e.g., by mandating standardized interfaces and continuous real-time portability, should be supported. It is, however, necessary to acknowledge also the limits of this data portability right and search for additional data portability solutions beyond the data portability right of Art. 20 GDPR.

12) Potentially difficult (but also limited) trade-offs between competition law and data protection law can arise through a) **competition law remedies for more data access** and data-sharing, and b) new forms of **anticompetitive behaviors that use privacy protection reasonings** for impeding the possibilities of competitors to get access to personal data. These cases need a deep analysis, the development of new approaches and tools, as well as the emerging trade-offs might be solved best by a collaboration of competition and data protection authorities.

IV. Policy conclusions: Introduction

13) The task of the policy part of this report is to ask for policy solutions which - with respect to the huge economic power of the large digital firms – answer the question how their market power can be limited, and the protection of personal data and informational self-determination can be strengthened. This requires **policies that address both the competition problems and the information and behavioral problems of the consumers**, i.e. their capability to

have control over and manage “their” personal data.Therefore, these firms should not only be subjected to stricter rules with respect to competition but also to stricter rules with respect to data protection and consumer law (**asymmetric regulation**).

14) **Two basic strategies** can be distinguished: One currently already much discussed option (basic strategy I) is to take privacy and data protection concerns more into account in competition policy (like, e.g. in the Facebook case of the German Federal Cartel Office). A second more far-reaching option (basic strategy II) is a more integrative and collaborative approach between competition policy, data protection law, and consumer law, which offers a much better perspective for solving conflicts and using and developing more synergies between these three policies for helping to solve both market failures.

15) The report analyzes the **range of possible policy solutions** in three steps:

a) How can privacy and data protection concerns be included in traditional competition law (basic strategy I)?
b) How does the Digital Markets Act (DMA) proposal deal with the relationship between competition policy and data protection policy, and how can it be improved with respect to more effectiveness regarding both competition and data protection?
c) How can outside of competition-related policies data protection law and consumer policy help to solve the problem of the huge economic power of large digital firms? This refers to the basic strategy II with its integrative and collaborative approach.

V. Traditional competition law

16) After the insight that traditional competition law might not be effective enough to deal with the economic power of the large digital firms, a broad consensus has emerged in Europe about the need that they should be subject to an **additional layer of stricter rules** for their behavior. This has led to the new sect. 19a GWB in German competition law and the proposals of new ex-ante regulatory approaches in the EU (DMA) and the UK ("pro-competition regime for digital markets").

17) **Competition law and privacy:**

a) Despite these new regulatory approaches traditional competition law will play also in the future an important role for addressing market power problems of large digital firms and should therefore also be improved with respect to its effectiveness.
b) Within the international competition law community, a lively discussion has emerged how data protection and privacy concerns can be better taken into account in competition law,

as part of the assessments in competition cases. These developments should be supported, which requires also much research in new methods and tools for assessing privacy effects.

VI. The "Digital Markets Act" proposal (DMA)

18) The Digital Markets Act with its **ex-ante per-se rule regime** for the behavior of gatekeeper platforms is intended to be the key instrument of the EU Commission for dealing with the economic power of the large digital platforms. It is complementary to traditional competition law but pursues also other objectives than Art. 101 and 102 TFEU. A large part of the report analyzes this proposal in a deeper way with the following results.

19) **Objectives of the DMA**:

a) The openness of the meaning of its objectives **"contestability"** and **"fairness"** has led to uncertainty, whether the DMA is only a different (ex-ante regulatory) form of competition policy or whether – related to the concept of fairness – it can pursue also other policy objectives, as, e.g., data protection and consumer policy objectives.

b) Since **consumers** are at least similarly dependent from gatekeepers as business users, they should be protected to the same extent as business users against unfair practices of gatekeepers.

c) The **fairness concept in the DMA** can be interpreted as encompassing different dimensions, as, e.g., a fair sharing of surplus, protecting the autonomy of business and end users (with strengthening choice), and protection against informational and behavioral manipulation (like, e.g. "dark pattern" behavior).

20) The **data protection and consumer policy dimension** of the DMA:

a) We propose to interpret the DMA as a regulation of large gatekeeper platforms that in addition to competition can also take into account data protection and consumer policy objectives.

b) This would lead to a more consistent interpretation of the DMA and its obligations and is in line with our general policy suggestion that the large digital firms need an asymmetric regulatory approach not only for competition but also for data protection and consumer policy.

c) The protection against **unfair restrictions of choice of end users** (through privacy policies and/or tying practices) in the obligations should be interpreted and enforced not only for supporting contestability but also with respect to strengthen data protection and consumer policy objectives.

d) Since nearly all obligations can be traced back to past and current competition cases, it is important to open the perspective that in future also **new obligations can be included** that focus much more directly **on data protection and consumer policy concerns**. It is therefore recommended that Art. 10 DMA about the update mechanism for obligations also clearly refers to unfair practices with respect to end users.

21) A deeper analysis of the obligations shows that they often cannot be explained well only from a competition-oriented interpretation of the DMA, i.e. that also separate and additional fairness criteria play an important role. Vice versa, a more **explicit acknowledgement of the data protection and consumer policy objectives** in the DMA could strengthen these aspects in the application, i.e. the further specification of the obligations.

22) Art. 5(a): **Combination of personal data**:

a) Most prominent for the relationship between competition law and data protection law is the obligation of Art. 5(a), which prohibits the gatekeepers to combine personal data from different sources without an additional consent of the end users (according to the GDPR). This corresponds to the **remedy in the German Facebook case**.

b) A deeper analysis of this obligation raises **serious concerns about its effectiveness** with regard to solving competition problems and the privacy risks through the information and behavioral problems of this additional consent. These concerns suggest that the current version of Art. 5(a) either aa) needs **additional rules for ensuring a meaningful choice** or bb) should be changed into a direct prohibition of the combination of personal data without giving the gatekeepers the option to get consent from the end users.

c) Since in our view the direct prohibition of the combination of personal data would have positive effects both for contestability and for privacy protection, we propose to change Art. 5(a) into a **direct prohibition of the combination of personal data** by the gatekeepers.

23) **Additional obligation for ensuring more choice regarding personal data**:

a) It is unclear if not being forced to consent to the combination of collected personal data (Art. 5(a) DMA) is a sufficient **minimum standard of choice** for consumers with respect to their control over “their” personal data. Why should consumers not have much more far-reaching options for choosing to what extent and for which purposes they allow the collection and use of "their" personal data by the gatekeepers as providers of core platform services?

b) From a data protection and consumer policy perspective it can be justified due to the large economic power of gatekeepers that also other obligations can be introduced, which give

the consumers much more and also granular choice about the provision of their personal data.

c) We propose to introduce an additional obligation that would **mandate the gatekeepers to offer the end users additionally the option to pay** for their core platform services **with a monetary payment instead of personal data** (e.g., a monthly subscription fee). This would eliminate that consumers are forced to "pay" with their personal data for services that they usually cannot avoid any more. Through additional measures (like fee regulation and subsidies) it can be ensured that all data subjects can afford to use such an alternative payment model.

24) We welcome that in a number of Art.5 and Art. 6 obligations (e.g. Art. 5(e), 6(1)b, 6(1)c and 6(1)e) the **freedom of choice of business and end users** is protected. We view these rights of business and end users not only as an instrument for enabling more competition but also as strengthening the autonomy of business and end users, which also should be explicitly taken into account in the process of further specification of these obligations.

25) All three obligations Art. 6(1)a, 6(1)i (**data access**), and 6(1)h (**data portability**) refer to the rights on those data that are generated by business and end users on gatekeeper platform services. Not allowing the platform to use these data for competing with the business users, and giving full real-time access and portability to business and end users regarding these data is justified at least as much by fairness than contestability, because it is a matter of fairness that those who generate the data should also be rewarded with its benefits. These rights protect the commercial opportunities of business users and the autonomy and empowerment of consumers.

26) Other obligations and rules:

a) Achieving more **interoperability** is a key strategy for enabling more competition and strengthening the freedom of choice of business and end users. We concur with many critics of the current version of Art. 6(1)f that this obligation is not far-reaching enough.

b) The obligation of Art. 6(1)j for sharing search data with other search engines can lead to more effective competition among **search engines** and many benefits and more choice for consumers. We have, however, concerns how gatekeeper can handle the trade-off between protecting personal data without substantially reducing the usefulness of these data for the competing search engines. Here a close collaboration between the Commission and data protection authorities might be necessary.

c) The effectiveness of all rights about protecting choice of business and end users can suffer from behavioral manipulation through **"dark patterns"** (biased choice architecture). We

welcome the proposals that demand an explicit prohibition of this and other forms of behavioral manipulation, e.g. as an additional obligation for the gatekeepers.

27) Regarding the **overall assessment of the DMA proposal**, it remains an open question, which of the three European models (DMA, sect. 19a GWB, or a future "pro-competition regime" in the UK) will turn out as the most effective solution, or to what extent they are capable at all to deal successfully with the huge economic power of the large digital firms. In the following, a few general recommendations are offered for improving the DMA.

28) **Per-se rules vs. flexibility**:

a) It is unclear to what extent the main advantage of this per-se rule regime, namely a fast compliance with all these obligations, can be realized in practice due to the need for more specification of these per-se rules. However, making too many concessions to demands for more flexibility endangers the entire rationale and effectiveness of this type of regulatory approach. Regarding this **difficult balancing problem between the advantages of strict rules and flexibility** we recommend to start with a fairly strict approach with not much flexibility, and to introduce only step-by-step (and after more experience) additional flexibility for a further refinement of the obligations.

b) Since the main problems are caused by the small number of the large digital firms, we recommend to design the quantitative criteria for **designating gatekeepers** in that way that primarily the core platform services of the large digital firms are addressed in the DMA. This allows for stricter rules and enforcement.

29) **Strengthening enforcement:**

a) In line with other commentators we also support strongly proposals that lead to a faster and stricter enforcement of the obligations. This also encompasses an **earlier and easier applicability of structural measures**, more human resources for ensuring effective compliance of the gatekeepers, and the building up of necessary technical expertise, and far-reaching investigative powers.

b) Due to the uncertainty about the success of this per-se rule regulatory model of the DMA, it is crucial that the architecture of the DMA can evolve over time, which might have to go beyond the current **update mechanism** regarding core platform services and obligations.

c) For the same reasons the DMA should be very careful not to preempt other innovative policy approaches that deal with the economic power of the large digital firms, and should be open to use the **expertise of other enforcement agencies**, also at the national level.

VII. The contribution of data protection law, consumer policy, and the perspective of a **more integrative and collaborative policy approach**

30) The basic strategy II that focusses on the combination of competition policy, data protection law, and consumer policy is in the center of the last part of the report. Data protection and consumer policy can also directly contribute with their instruments for helping to solve the problem of the economic power of the large digital firms. It can be asked what these policies can do better unilaterally, and, in an additional step, what can be done in a more integrative and collaborative approach between all these policies, especially also with respect to strengthen synergies between the policies.

31) **Data protection and asymmetric regulation:**

a) In principle, the GDPR follows a "one-size-fits-all-approach", i.e. all firms are treated equally. Nevertheless, a **risk-based approach** underlies some of its provisions. We are of the opinion that the risk-based approach should be a basic principle of the GDPR, meaning that the GDPR should set a minimum standard for every data controller and that the more significant the risk, the stricter the obligations should be.

b) This risk-based approach could be realized not only by asymmetric regulation but also by interpreting the GDPR and evolving guidelines (e.g. for the application of Art. 6(1)f and Art. 6(1)a GDPR) which take into account the risk which lies in the data processing and the data controller.

c) The two market failures justify a rebuttable presumption of invalid GDPR consent if the consent is given to very large online platforms which needs to be refuted e.g. through a paid option to use the platform.

32) If especially **dangerous data processing by very large online platforms** is identified, one could even think about prohibiting this data processing at all as long as the information market failure is not solved. If the risk for the data subject clearly outweighs the interests in data processing and the concept of consent does not work due to the two market failures, the need to protect the data subject justifies a prohibition of highly dangerous data processing.

33) Data protection law can help to reduce dark patterns. Where **biased choice architectures** influence data subjects to declare consent to data processing, e.g. by using green buttons to give consent whereas the button to deny consent is colored red (preselection patterns), one could think of an (in)voluntarily given consent. California has implemented a law (1798.140 lit. h Cal. Civ. Code) providing that consent to data processing obtained by means of dark patterns shall be invalid. A similar law or, in any case, a respective interpretation of the GDPR, could

be part of the "**dark pattern solution**" in Europe, too. We support such a law and such an interpretation of the GDPR.

34) **Solving better enforcement problems of the GDPR**:

a) The enforcement deficit of data protection law lies, on the one hand, in the legal uncertainty inherent in data protection law and, on the other hand, in the lack of enforcement efforts by individual data protection authorities. This, in turn, may be due to a lack of resources, but certainly also to other reasons, most notably the effects of the **"one-stop-shop principle"** and the resulting complex structure of competency.

b) Although the "one-stop-shop-principle" may cause more legal certainty, it leads to inconsistent law enforcement in the different member states. We thus argue in favor of a financially adequately equipped **European Data Protection Authority** which is competent for the data processing by very large online platforms. To identify potentially unlawful data processing, one could also think of **further reporting requirements**, e.g. within the scope of Corporate Digital Responsibility.

35) **Consumer policy:** With its wide range of instruments for dealing with information and behavioral problems of consumers, consumer law might be an important policy for better solving these problems on digital markets. However the new challenges (e.g. dark patterns) require new policy initiatives. In that respect, also asymmetric regulation in form of stricter rules for the largest digital platforms can be justified.

36) **Towards a more integrative and collaborative approach:** Due to the deep intertwinement of the effects of competition law, data protection law, and consumer policy on competition, data protection and consumer empowerment, a stronger integrative policy approach that enables some form of coordination and collaboration between these policies would offer the chance of more effective solutions for dealing with the huge economic power of the large digital firms. More coordination and collaboration is also very important between the **enforcement agencies** of these policies.

1. Introduction

The large digital firms (or tech firms)[1] Google, Facebook, Amazon, Apple (and to a lesser degree Microsoft) are in the center of intense policy discussions in many countries with respect to the problem how their huge economic power can be limited, especially with respect to their market power on digital platforms that threatens competition, innovation and consumer choice. The current discussions about very far-reaching reforms in competition policy, as e.g. the "Digital Markets Act" proposal of the EU Commission,[2] reflect the great challenge that these firms pose to the economy and society. Through the analysis of the power of these digital platforms it became increasingly clear how deep the collection and use of vast amounts of personal data by these firms (especially for targeted advertising on digital advertising markets) is linked and intertwined with their economic power. The reason is that this data power can again lead to large competitive advantages on many markets and at the same time might also allow them to influence the behavior of consumers through informational and behavioral manipulative strategies. Through the combination of market power and information power the users of the core platform services of these large digital firms might not be capable anymore to have meaningful control over their personal data, leading to serious dangers for their informational self-determination and privacy. As a consequence, this economic power of the large digital firms is also a great challenge for data protection law.

This has led to the insight that on digital markets the issues of competition and data protection, and therefore competition law and data protection law are deeply intertwined with each other. Therefore, it is not surprising that the Facebook case of the German Federal Cartel Office[3] has triggered an international discussion about the relationship between competition law and data protection law in the digital economy. Partly linked and partly independent from this discussion about the economic power of the large digital firms, it has been also discussed for some time, whether and to what extent the EU data protection law (GDPR), which is viewed as a strict regulation for protecting the personal data of EU citizens, might also erect too many hurdles leading potentially also to negative effects on competition and innovation. Therefore, the question has emerged about potential tensions and even conflicts between competition

---

1 In this report we use for these firms the term "large digital firms" (in line with the German term "große Digitalkonzerne") instead of the often used "large tech firms" or "large digital platforms". The latter does not fit well, because these large digital firms have a much more complex conglomerate structure, which also consist of digital platforms.

2 European Commission (2020a). Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

3 Federal Cartel Office (2019). Decision no B6-22/16 of 6 February 2019.

and data protection law. For example, the question has been raised, whether the GDPR might even lead to a strengthening of the economic power of the large digital firms. This would be another important aspect with respect to the new relationship between data protection law and competition law under the new economic and technological conditions of the digital economy.

The task of this report is to analyze, especially with respect to the economic power of the large digital firms, the relationship between competition law and data protection law, and assess and develop policy strategies and proposals that might help to achieve better the objectives of both competition policy and of data protection law. This will require an integrated analysis of the competition and data protection problems on digital markets, and the impact of both competition law and data protection law on competition and data protection (and privacy). We are very much aware that there is a broad discussion in German data protection law if and to what extent data protection law protects the right to informational self determination and to what extent it is based on Art. 7 and/or 8 GrCh and therefore also refers to privacy protection or not. However, this discussion is not representative for the discussion in Europe outside of data protection law. The intertwinement between competition aspects and problems concerning the use of personal data are internationally discussed very well with regard to privacy as a whole. Therefore, we also want to discuss the dangers for privacy as a whole, not only for data protection law or the right to informational self-determination. This is why our argumentation faces both, the risks for privacy at all and the right to informational self determination in particular.

To what extent do tensions and conflicts between competition law and data protection law exist, and to what extent can both legal regimes work into the same direction of more competition and more choice for consumers and informational self-determination? What policy proposals can be made for strengthening synergy effects and mitigate conflicts between competition law and data protection law?

The report consists of two parts:

(1) The first part (chapter 2) offers a "mapping" of the competition and data protection problems through the economic power of the large digital firms, and of the new complex relationship between data protection and competition law on digital markets. This also includes an analysis of selected tensions and synergies between both legal regimes. Important results will be (a) the need of an integrated analysis of both policies with implications for also a more integrative and collaborative policy approach, and (b) the proposal that the large digital firms should be subject to asymmetric regulation not only with respect to competition but also data protection and consumer policy.

(2) The second part (chapter 3) has the task to assess and develop policy solutions with respect to the economic power of the large digital firms, which simultaneously foster competition and data protection (synergies). Since the current policy discussion focuses much on competition policy, traditional competition law and, to a much larger extent, the current "Digital Markets Act" proposal are analyzed with respect to the question, how they can include also data protection and consumer protection concerns. This will lead also to a number of recommendations for improving the DMA proposal. Particularly important will be our recommendation that the DMA should consider much more explicitly also data protection and consumer policy objectives. In the last part of chapter 3 we also ask outside of competition-related policies how data protection law and consumer policy can directly contribute more to solving the competition and data protection problems through the large digital firms. This, finally, will lead to the proposal of a more coordinated and collaborative approach between competition law, data protection law, and consumer policy.

2. Data protection law and competition law: A mapping of the relationship, conflicts, and synergies

2.1 Economic Power of large digital firms, competition, and privacy: What are the main problems?

Although it is broadly acknowledged that the large digital firms Google, Amazon, Facebook, and Apple (often called GAFA or large tech firms) have been key drivers of innovation in the digital economy, also the concerns about their huge economic power have increased dramatically in recent years. A large number of competition policy reports, published 2018 and 2019, have led to a broad reassessment of the power of these firms.[4] These reports show a great consensus that (1) digital platform markets, as, e.g., search engines, social media services, and other platform services are characterised by very large economies of scale, and direct and indirect network effects that can lead to one dominating platform ("tipping"). (2) The collection and use of data, especially also personal data of consumers, plays a key role for the market power of the providers of these platform services. Particularly important is that the large digital firms do not only offer such platform services (with "winner takes all" implications) but also have built up complex digital ecosystems, which offer a multitude of complementary services to the consumers with lock-in effects and high switching costs ("walled gardens"). Important is that the market power of these digital firms is, in the meantime, so entrenched and persistent that it is seen as very improbable that their market position can be challenged in the near future. This is also caused by high entry barriers, e.g. also through their superior access to data, but also through the strategy of acquiring many new, fast-growing innovative firms that might have been capable of challenging the incumbent digital firms.

These entrenched and persistent market positions can lead to manifold negative effects on competition, innovation, and consumer choice. Although nobody would deny that the large digital firms are still innovative, they increasingly use their economic power, their data, and their superior capabilities with respect to data analytics, algorithms and AI for expanding their market power positions in the digital economy. Through a number of strategies, like tying services or self-preferencing, these firms can leverage their market power to other markets (envelopment strategies). These strategies can lead to exclusionary effects on many other firms and impede their innovative activities. Through the offering of quasi-monopolistic core platform services (e.g., search engine services and social media services) these large digital firms are

[4] See Schweitzer et al. (2018), Crémer et al. (2019), Furman et al. (2019), ACCC (2019), Stigler Committee on Digital Platforms (2019), and Wettbewerbskommission 4.0 (2019); for overviews about these reports see Kerber (2019) and Lancieri/Sakowski (2021).

often in gatekeeper positions between different market sides, which allow them to use unfair and exploitative practices vis-a-vis both the business users and the end users (consumers) of these platform services. Therefore a broad discussion has emerged that the business users, e.g. on intermediation platforms (like Amazon market place) or advertisers on digital advertising markets (with Google and Facebook as dominant firms), are subject to unfair business practices by these platforms with negative effects on competition and innovation. Through the quasi-monopolistic market structure with regard to these core platform services, also the consumers can be harmed through less competition, choice and innovation.[5] The main additional problem of excessive collection and use of personal data of consumers by the large digital firms will be discussed below.

The common conclusion of these reports (and in the meantime also of many policy-makers) is that the economic power of these large digital firms is a very large **unsolved competition problem**. Since the traditional competition law with its ex-post control of abusive behavior (like Art. 102 TFEU) does not seem to be capable of dealing in an effective way with this huge challenge, it is widely seen as necessary to search for **new approaches in competition policy**. This has led to the current proposal of a new ex-ante regulation for gatekeeper platforms by the EU Commission ("Digital Markets Act") or the new sect. 19a GWB in the recent amendment of German competition law.[6]

However, the digital economy has also led to a second huge and unprecedented challenge, namely the **new dangers to the privacy of persons** (consumers) and their right to make meaningful decisions about the collection and use of their personal data (informational self-determination). In particular, Google and Facebook collect a large amount of personal data through their manifold services, as the search engine, social media, and other services, which are offered for a monetary price of zero ("free") to the consumers but for which they have to “pay with their personal data”. However, “paying (fully or partly) with personal data” is not limited to the large digital firms but a wide-spread practice in the digital economy. While the provision of personal data of consumers to firms can also lead to benefits for the consumers (for innovation, improvements, and personalisation of services), it can also lead to a wide range of new risks and potential harm for consumers (e.g. through price discrimination, identity theft, fraudulent and manipulative practices, and profiling).[7]

---

[5] For an easy-to-read and clear summary of all these competition problems and their potentially harmful effects, see chapter 1 of the Furman report (Furman et al. 2019, 17-53).

[6] See Furman et al. (2019, 5) for the need for an additional ex-ante regulatory approach. For the discussion about new approaches and the DMA proposal see below sections 3.2 and 3.3.

[7] See for a brief overview about the risks OECD (2020, 22)

The basic approach in EU data protection law is that consumers (as data subjects) have the right to control the processing of their personal data by giving voluntary and informed consent (according to Art. 6(1)a GDPR), i.e. that they should be able to decide, which personal data are collected and used by whom and for what purposes (informational self-determination). However this instrument of "notice and consent" does not work well, because consumers are overwhelmed by too many decisions about consent, with often intransparent and hardly comprehensible and lengthy privacy policies, especially in combination with manipulative behaviors of the data-collecting firms.[8] As a consequence, consumers are not capable of managing their personal data in a rational and well-informed way. This endangers their consumer sovereignty and informational self-determination, and impedes their capabilities to protect their privacy.[9] This is a general problem on many consumer-oriented markets in the digital economy, on which firms are collecting personal data from the consumers. It is caused from an economic perspective primarily through the **market failure of information and behavioral problems**, which is not sufficiently solved by data protection law (or consumer law).

However, it is a particularly serious problem with respect to the large digital firms. Since, e.g. Google and Facebook offer with their search engine or social media platform services that are de facto non-avoidable for most consumers (due to the lack of realistic other options; "must-have" services[10]), these large quasi-monopolistic digital firms have the possibility to collect vast amounts of personal data from their users. In addition, these firms also have manifold possibilities to collect personal data via third-party websites and through tracking the consumers all over the internet.[11] Therefore the combination of information and behavioral problems and the market power problem leads to the danger of excessive collection of personal data, which might not only be an exploitative abuse of market power but is also a huge problem for the informational self-determination and the protection of privacy. Consequently, we have through the large digital firms an **unsolved privacy problem**, which is a **huge challenge for data protection law**.

For the relationship between competition law and data protection law it is of utmost importance that this **competition problem is deeply linked to this privacy problem**, because it is, on the one hand, the economic characteristics of the platforms with their monopolistic tendencies, which allow the providers of these core platform services to collect so much personal data due

8 See below in section 2.3.1.

9 See SVRV (2021, 370 ff.), Datenethikkommission (2019, 96), and Wettbewerbskommission 4.0 (2019, 43), Solove (2013).

10 See CMA (2020a, 4.120)

11 See ACCC (2019, 84-87), Binns/Bietti (2020), CMA (2020a, 2.18-2.22).

to the lack of choice for consumers. On the other hand, this superior access to personal data can lead to the further entrenchment of the economic power of the large digital firms through (a) increasing barriers to entry and foreclosing competitors (e.g. on markets for digital advertising), and (b) through manifold possibilities to use this large information asymmetry between them and the consumers in manifold ways for their informational and behavioral manipulation.[12] It is this key role of personal data for the core markets of the large digital firms, which leads also to the **deep linkage between the problems for competition policy and for data protection law**.[13]

The famous Facebook case of the German Federal Cartel Office (FCO),[14] in which for the first time a data-collecting behavior of a digital firm was prohibited in 2019 as an abusive behavior of a dominant firm in a competition case, is a very innovative pioneer case: It focusses exactly on this linkage between the competition problem and the privacy problem with respect to Facebook as one of the large digital firms. In this case the FCO argued that due to the dominant position of Facebook on the German market for social media platform services forcing the users of these services to give consent to the merging of personal data that Facebook has collected from different services in and outside of Facebook infringes EU data protection law and is therefore an abusive behavior of a dominant firm. It imposed the remedy that Facebook has to give an additional choice option with respect to the merging of these personal data for protecting the privacy of the consumers, but also to mitigate the anticompetitive effects through the data advantages of Facebook with regard to its competitors. With this unprecedented linkage between competition law and data protection law the German FCO has triggered a new world-wide discussion about the relationship between competition law and data protection law.[15]

12 See Digital Regulation Project (2021a, 10).

13 See Douglas (2021, 3), Kerber (2021d).

14 See for the German Facebook case Federal Cartel Office (2019), Robertson (2020), Podszun (2020), and from an economic perspective Kerber/Zolna (2021).

15 See as recent overviews OECD (2020), Douglas (2021)

2.2 Competition law, data protection law, and consumer law: A legal and economic policy framework

Section 2.1 showed that both competition policy and data protection law face huge challenges through the digital transformation and, in particular, the economic power of the large digital firms. We also have seen that through the key role of personal data on many digital markets both problems – the competition problem and the data protection problem – are deeply intertwined with each other. This is also a consequence of the fact that from an economic perspective these digital platform markets suffer – with respect to the collection and use of personal data – simultaneously from two different market failures, namely the market power of the platforms and the information and behavioral problems of the consumers. We claim that a deeper understanding of the relationship between competition law and data protection law requires an approach that allows for an integrated analysis of the effects of both market failures and both legal regimes. This also would allow for a much better analysis of potential conflicts and synergies between both laws. This section 2.2 will therefore present such an analytical framework, which can also contribute to the development of more effective strategies for policy solutions in chapter 3 through its provision of a map for analyzing the interplay between competition law and data protection law.[16]

The framework is based upon an economic policy approach, which focuses on solving market failure problems and views policies as instruments for achieving normative objectives and protecting fundamental values of the society.[17] From that perspective competition policy has the task of solving the market failures with regard to competition. Data protection law has the task of protecting the right to informational self-determination. This is done from an economic perspective by defining rights of natural persons (data subjects) with respect to “their” personal data, but also by setting up rules about how, e.g., firms (as the large digital firms) can collect and use the personal data of consumers for certain purposes, in particular through (but not limited to) the consent of the data subjects. However, due to the very serious information and behavioral problems of consumers, the requirement of a well-informed consent is often not fulfilled. From an economic policy perspective the solution of the market failure "information and behavioral problems" is usually the task of consumer policy, but with respect to the collection and use of personal data it is primarily the task of data protection law. Therefore both data

16 See for this analytical framework and how it can be used Kerber/Zolna (2021) and Kerber (2021d).

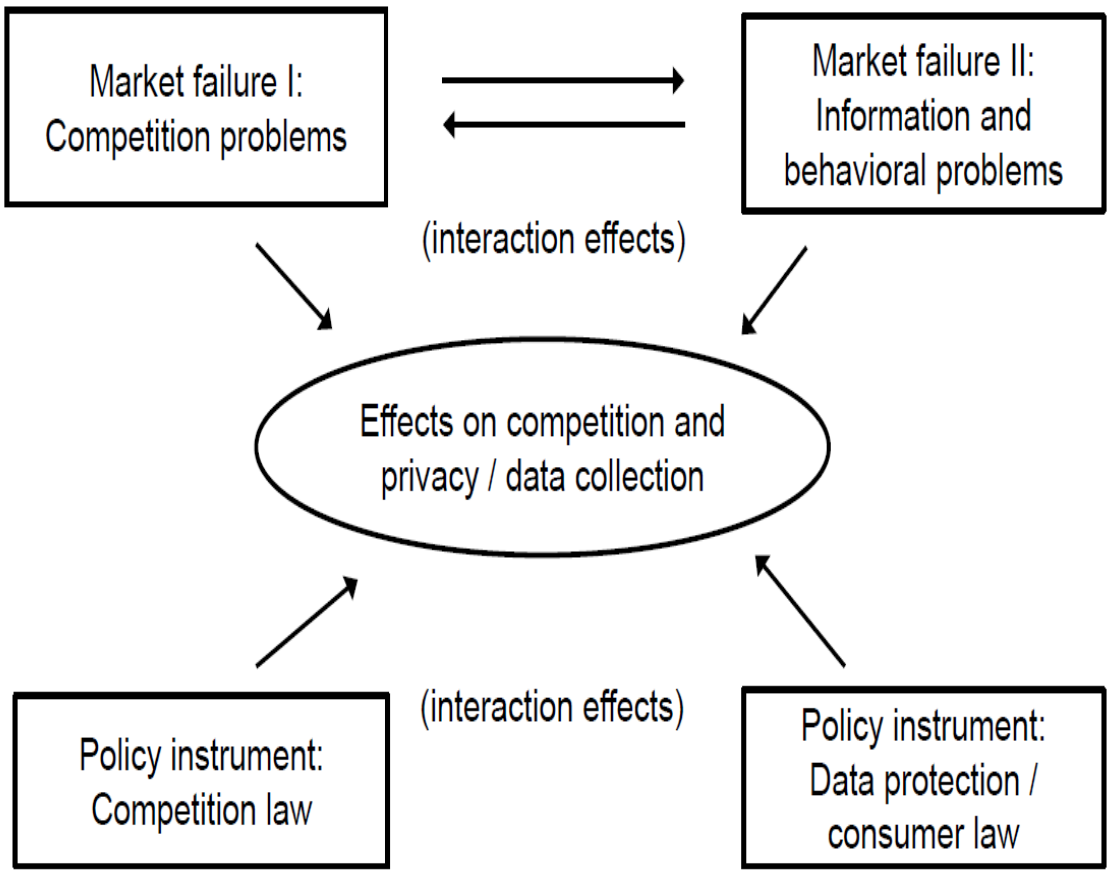
17 See, for the following, Kerber (2016) from an economic perspective. For a comparative analysis of competition law, data protection law, and consumer law from a legal perspective, which analyzes their similarities and differences also with respect to the relationship between these different policies, see Costa-Cabral/Lynskey (2017), Helberger et al. (2017), Graef et al. (2018).

protection law and consumer law should help enabling the consumers to make well-informed decisions about their personal data. This would empower consumers and strengthen their consumer sovereignty and informational self-detemination, and therefore facilitate the protection of their privacy.

For a long time, competition law and data protection law have been seen as entirely separate policies with different objectives and the task of dealing with different market failure problems. This is the reason why this innovative Facebook case of the German Federal Cartel Office has been so controversially discussed: It took into account privacy concerns in a competition case and linked it directly with data protection law. Therefore it is not surprising that the main critique of the FCO decision in this case came from the traditional approach that these two legal regimes should be kept separate, i.e. that competition law should focus on the protection of competition, and data protection law should deal with privacy problems.[18] Also the EU Commission has held the view that privacy concerns should be dealt with by EU data protection law and not by EU competition law, which up to today leads to a very cautious approach in EU competition law with respect to considering also privacy effects in competition cases.[19] However the discussion about the economic power of large digital firms has led to the insight that there are manifold interdependencies between both legal regimes, and that therefore such a pure separation approach is not a suitable and prudent strategy any more, particularly on digital markets that are dominated by these large digital firms, where both significant market power and information asymmetry problems exist. In contrast to the traditional separation model, which had implicitly assumed that there are no significant interdependencies between these two policy regimes, Figure 1 (next page) shows a much more complex picture with multiple interdependencies between the effects of the market failures and these policies. In the following, this will be explained step-by-step.[20]

[18] See for this separation thesis in the Facebook case Körber (2019), Kellezi (2019).
[19] See Volmar/Helmdach (2018), OECD (2020, 26-29), Robertson (2020, 187).
[20] See for the following also Kerber/Zolna (2021, 8-12).

Figure 1: Two market failures, two policies, and their interaction effects[21]



First, we can look at the effects of the two market failures:

(1) The serious problems of the consumers to manage their personal data through large information problems and potentially manipulative strategies of digital firms cannot only have negative effects on privacy and informational self-determination but also impede competition, because consumers cannot compare well the privacy policies of different firms.[22]

(2) Vice versa, the market power of large digital firms on their core platform markets does not only imply lack of competition but can also directly have negative effects on privacy and informational self-determination, e.g. through excessive collection and use of personal data or not allowing genuine choice.[23]

---

21 See Kerber/Zolna (2021, 10)

22 See below section 2.3.1.

23 See about the problem of excessive data collection Robertson (2020), Economides/Lianos (2021); see for the lack of genuine choice ACCC (2019, 22-23) and Condorelli/Padilla (2020, 181).

(3) Particularly important is that also the combination of both market failures can further increase the economic power of the large digital firms, partly because these market failures can mutually reinforce each other, and partly because the combination of market power and information power can have additional negative effects on both competition and privacy.[24]

Secondly, also the effects of the two policies can be analyzed. As well as competition law on digital markets can- not only have effects on competition but also on privacy, vice versa, also data protection law does not only have an impact on the right to informational self-determination but can also have effects on competition:

(1) Positive and negative effects of competition policy on privacy:

(a) If, for example, competition law does take into account negative effects on privacy in merger cases, e.g., through limiting the effects of the combination of sets of personal data of the merging firms, then merger policy can have positive effects on privacy, and therefore support data protection law in ensuring a high level of data protection.[25] The same is true, if competition law would prohibit horizontal agreements between competing firms, if these agreements restrict competition for privacy-friendly policies with respect to the collection and use of data. The example of the German Facebook case shows that also the control of abusive behavior of dominant firms with its remedy of an additional choice can have positive effects on privacy and informational self-determination.

(b) Competition law can, however, also have potentially negative effects on privacy. Particularly important are in that respect remedies about data access and data-sharing for solving competition problems and reducing entry barriers through data advantages of incumbents, if these data also encompass personal data. Here, a direct conflict might arise, because data protection law might limit the scope of data-sharing, especially through the requirement of the consent of the data subjects, and therefore reduce the effectiveness of this competition law remedy.[26] Another problem are the currently much discussed strategies, especially of the large digital firms, to limit the access to personal data by apps and third-party trackers, which might have negative effects on competition but perhaps also lead to more protection of privacy.[27] If

---

[24] The effects of the combination of both types of power has been analyzed also in Schweitzer et al. (2018, 99), where the link between intermediation power and information manipulation power is discussed. See also Digital Regulation Project (2021a, 10).

[25] See for the analysis of merger cases with regard to privacy effects OECD (2020, 25-29), Douglas (2021, 82-98).

[26] See below in section 2.3.4.

[27] See below in section 2.3.4.

competition law prohibits such strategies as anticompetitive, this might have in some cases negative effects on privacy.

(2) Positive and negative effects of data protection law on competition:

(a) If data protection law (and/or consumer law) would help to solve better the information problems with respect to the collection and use of personal data by digital firms or can prohibit certain forms of manipulative "dark pattern" behavior, then this can have positive effects on competition between firms,[28] especially also with respect to privacy-friendly terms with regard to personal data. Also the data portability right of Art. 20 GDPR has always be seen as a policy instrument in data protection law that has also the task of supporting competition through a reduction of switching costs between digital firms and platforms.[29]

(b) However, there is also an intense discussion about the question whether the high requirements of the GDPR with respect to the consent of data subjects for processing their personal data might have negative effects on competition, and would, in particular, favor large firms, who might get easier consent from consumers than smaller firms. This is also linked to the question whether the GDPR might make it more difficult to share personal data with other firms compared to the use of personal data within large diversified conglomerate firms.[30]

These manifold examples of effects of these two market failures and two policies on both competition and privacy show the importance of the analysis of the interplay between both policy regimes within such an integrated analytical framework. Additionally, three other aspects are important:

(1) The objectives of competition and data protection law also overlap to some extent, because negative effects on privacy (e.g. through larger privacy risks) can to some extent also be understood as consumer harm, and therefore can also be directly taken into account in competition law (with its consumer welfare standard). This has already been discussed for some time in competition law.[31] Also the problem of excessive data-collection can be dealt with as part

---

28 See, e.g., also Heidhues et al (2021) who show that in the case of a limitation of the attention of consumers, regulating secondary features of complex products through consumer law can have pro-competitive effects.

29 See below in section 2.3.3.

30 See below in section 2.3.2.

31 See for privacy as a part of the quality parameter of competition Stucke (2018, 285-290), Esayas (2018), Douglas (2021, 62-74). See for an analysis of legal scholars that the objectives of competition law and data protection law can overlap Coste-Cabral/Lynskey (2017) and Graef et al. (2018).

of the control of exploitative abuse of dominant firms, even if clear criteria and methods are still missing how to do this practically in competition cases.[32]

(2) Another important question refers to the availability of effective remedies for solving the competition and data protection and privacy problems. If the problems with large digital firms are caused by a combination of these two market failures, then competition law might run into the problem that it usually cannot apply remedies for solving information and behavioral problems, as well as, vice versa, data protection law (and also consumer law) do not have the option to apply remedies for solving competition problems, even if those have negative effects on privacy.[33]

(3) Also the effectiveness of the enforcement regimes of both policies might be important. If one of the policies has serious problems with regard to enforcement, like it is discussed for the EU data protection law (in particular, vis-a-vis the large digital firms),[34] then these enforcement deficits also can play a significant role for the relationship between competition law and data protection law on digital markets, and what both policies can contribute with respect to the economic power of the large digital firms.[35]

These examples of interaction effects between both legal regimes and these additional aspects like over-lapping objectives, available remedies and enforcement problems show the complexity of the relationship between competition law and data protection law.[36] Searching for effective solutions for the competition and data protection problems caused by the large digital firms therefore requires to take these interaction effects and the ensuing complexity into account.

If in situations with such complex interaction effects both laws are applied independently from each other (as this has been done traditionally and still is the case with competition law and data protection law), then the following three problems can emerge:

---

32 See Robertson (2020).

33 See Kerber/Zolna (2021, 15).

34 See below in sections 2.3.2 and 3.4.2.

35 The fact that the German FCO has prohibited a behavior that infringes EU data protection law has always raised the question, why this behavior was not prohibited directly by a data protection authority. This can only be explained by the enforcement problems of EU data protection law. This is supported by the fact that data protection authorities welcomed the decision of the German FCO.

36 See for an international analysis of the intersections between competition laws and privacy laws and the complexity of this relationship, in particular, Douglas (2021): "Antitrust and data privacy law are meeting in complex and multi-faceted ways, particularly in the digital economy. Despite often being summarized as complementary or in tension, the relationship between antitrust law and data privacy law is more nuanced. A closer examination reveals a landscape of multi-faceted interactions, many of which are only beginning to be recognized and understood." (ibid. 3).

(1) Conflicts: The application of the laws might lead in certain cases to conflicts between both legal regimes, as in the case of competition law remedies that would mandate the sharing of personal data with its potential negative effects on privacy.[37]

(2) Gaps: There might also be important cases, in which a problematic behavior with negative effects on competition or privacy is neither addressed by competition law nor data protection law, because both laws deem these effects as being beyond the scope of their tasks. Large gaps can also emerge, if one of the policies is only insufficiently enforced.[38]

(3) Synergies: Particularly important are the manifold possibilities, in which the application of both laws work into the same direction, i.e. supporting competition and privacy. Then the question can be asked what policy solutions can help to improve the use of these synergies or create new ways, how competition law and data protection law can help each other for achieving their objectives.[39]

Therefore, the task of searching for policy solutions can also be put as follows: How to solve or at least mitigate conflicts? How to close gaps? How create new or exploit better existing synergies between competition and data protection law?

What are basic policy options for dealing with these problems that arise through this deep intertwinement of competition law and data protection law? First, we should remind ourselves that these problems do not emerge generally between competition law and data protection law. Instead they are particularly important only on those digital markets, on which personal data play an important role, and on which we have serious competition problems and/or information and behavioral problems (as, in particular, with respect to the large digital firms). In such cases, however, it is clear from an economic policy perspective that an independent application of both laws, which does not take into account these interaction effects, will lead to unsolved conflicts, gaps, and an under-exploitation of potential synergy effects.

Then two basic policy strategies can be used for dealing with these problems:

(1) Unilateral strategies: The controversial debate that has been triggered by the German Facebook case has already led to a new discussion in the competition policy community to what

---

[37] Another form of conflict, which we are not analyzing, can arise, if competition and data protection authorities would make decisions that are not compatible with each other.

[38] The German Facebook case can also be understood as a case, in which a gap existed, because EU data protection law did not enforce the GDPR in such cases, and then the German FCO stepped in instead, and helped to close an existing gap.

[39] See for analyses of synergies and tensions between competition, data protection and consumer law from a legal perspective also Graef et al. (2018).

extent and how privacy can be better taken into account in competition policy.[40] Since privacy harms can to some extent also be seen as consumer harm in competition law, and certain (e.g. excessive) data collection strategies of large digital firms can also lead to anticompetitive exclusionary effects and increase entry barriers, there is considerable scope for taking into account also privacy effects in competition law. Therefore, one policy can also unilaterally try to take into account these interaction effects and help to achieve better competition and privacy. Such a discussion already exists in competition law and also in data protection law there are cautious tendencies to take competition law arguments more into account, at least in some regulations.[41]

(2) Coordinated strategies: Although such unilateral strategies might be capable of solving some of the problems, the effectiveness of such strategies will always be limited and run into serious problems, e.g. with respect to mitigating conflicts or finding sophisticated ways how synergies between both legal regimes can be used. Therefore a more coordinated approach between both legal regimes, which also might have to include some form of collaboration between enforcement agencies, might offer additional and more effective options for solving conflicts, closing gaps, and using better the potential synergies between both policies. This can refer to the use of remedies from competition law and data protection law in specific cases, but imply also a better alignment at the level of both laws, i.e., competition law and data protection law.[42]

This framework with the two market failures, two policies, and the interaction effects between them will be used throughout the entire report, both for the further analysis in this chapter 2 about the "mapping" of this relationship between the two legal regimes and, in particular, also in chapter 3 about policy solutions. In the remaining parts of chapter 2, we will analyze some particularly important and often controversially discussed questions about these interaction effects, conflicts, and synergies in more detail.

---

40 See the overviews about this discussion in OECD (2020, 24-41) and Douglas (2021).

41 See e.g. the discussion whether market dominance should be taken into account as part of the assessment of the requirements for valid consent in Botta/Wiedemann (2019, 439). This approach finds limited support in the Art. 29 Data Protection Working Party Opinion about legitimate interests of data controllers, in which the dominant position of a company on the market is also briefly mentioned as one of the factors that can be considered (Art. 29 Data Protection Working Party, 2014, 40). See also below in section 2.4.

42 See OECD (2020, 49-51) and Kerber (2016, 866).

2.3 Competition law and data protection law: Some synergies and conflicts

2.3.1 Competition, privacy, and the market for personal data

2.3.1.1 Does competition lead to more privacy?

One of the basic questions with respect to the relationship between competition law and data protection law is whether we can expect that more competition on a market, e.g. through a lower firm concentration or lower barriers to entry, would lead to a better protection of privacy, e.g. through less collection of data or more privacy-friendly terms with regard to the collection and use of personal data. What do we know about the relationship between competition and privacy? The problem is that there are still few empirical studies about this question, which also have so far led only to inconclusive results whether a more competitive structure in a market would lead to better terms in the privacy policies of the firms or to a lower level of collection of personal data.[43] Therefore the expectations that competition would have positive effects on privacy have not been fulfilled so far. On the contrary, data protection still seems to have only a low importance on many consumer markets. How can this be explained? In the meantime, we have ample evidence that one of the possible explanations, namely that consumers generally do not care about their privacy and the collection and use of their personal data, is not true. Consumer worry about their personal data and their privacy but they seem to have large problems in managing their personal data.[44] Based upon theoretical and empirical research we will show in this section that the market failure "information and behavioral problems" of consumers can explain why competition with privacy-friendly terms and conditions in the privacy policies of the firms does not work well, and why therefore the potential synergies from competition to privacy could not have been realized so far.

Based upon economic theory about markets we would expect that under competition firms would offer products and services that try to fulfill the preferences of the consumers. This also would imply that firms also compete with their privacy policies, and therefore would have incentives to adapt them to the preferences of the consumers. Since, however, on many digital markets the provision of personal data by the consumers is also used as payment for services ("data as counterperformance"), the decisions of the consumers have gotten much more complex: For comparing the privacy policies of different firms the consumers have to take into

---

[43] See for an overview about the complex relationship between competition and privacy, including various hypotheses how competition can impact privacy, and the scant existing evidence through empirical studies Blankertz (2020). See as examples with different results that hint to opposite effects Kesler et al. (2019) and Sabatini/Sapi (2019).

[44] See Blankertz (2020) with further references regarding surveys of consumers.

account also the "data price" they are paying for this service (in terms of allowing the firms to collect and use their personal data), and whether the value of this service is higher than this "data price". This would require not only information about what data are collected and for what purposes they are used, but also an assessment of the value of these data as well as the "costs" of providing these data in terms of the additional risks through the provision of these data.[45] Since revealing personal data to others cannot only lead to additional privacy risks, which might harm the consumers in the future, but also might increase the benefits for the consumers through a personalisation of these services, a well-functioning market, in which consumers pay with their personal data, requires very complex and difficult assessments by the consumers about the benefits and costs of such a trading of "personal data for services". If consumer do not have this information and cannot make these assessments, then even rational consumers cannot distinguish, which privacy policies fulfill better their preferences, and cannot take them into account in their consumer decisions, which again will eliminate the incentives of firms to provide more privacy-friendly terms and services. As a consequence, it cannot be expected that privacy policies are a very relevant parameter in competition. Therefore already the use of simple microeconomic theory shows us that for making correct decisions about the providing of personal data on digital markets by consenting to privacy policies, high requirements with respect to information and assessment capabilities of the consumers have to be fulfilled, even if they act fully rational and do not suffer from behavioral biases.

2.3.1.2 Information and behavioral problems of consumers and the problem of "dark pattern" behavior

Art. 6 (1) a GDPR requires that the provision of personal data to firms is based upon "notice and consent" solutions, i.e. the firms are supposed to give information about the data they are collecting, and for what specific purposes they are using these data, and based upon this information the data subjects decide whether they give their consent for this processing of their personal data. This consent about the processing of personal data has to be a "... freely given, specific, informed and unambiguous indication of the data subject's wishes ..." (Art. 4(11) GDPR).[46] However also in the law an increasingly critical discussion has emerged that these "notice and consent" solutions might not work effectively as an instrument for the consumers to make meaningful decisions about giving consent regarding the collection and use of “their” personal data.[47]

---

45 See Acquisti et al. (2016).

46 See also the guidelines on consent of the European Data Protection Board (2020).

47 See, e.g., Luzak (2014).

In section 2.1 we already claimed that consumers are not capable of managing their personal data in a rational and well-informed way. In the following, we will analyze in more detail the manifold problems that consumers have to face in making these decisions for managing their personal data on digital markets:[48]

(1) Data-collecting firms are often not transparent enough or give misleading information about what data they collect and how they are using them, and with which firms they are sharing the data (and, again, how these firms use these data). The privacy policies also often use very broad and general terms, which do not provide specific information.

(2) Additionally, firms can also collect personal data secretly without informing the consumers. A particular complex problem are the manifold ways of tracking consumers in the internet, which is very intransparent for consumers.

(3) The privacy policies of data-collecting firms are often very long and incomprehensible for consumers. This leads to too high information costs, i.e. it is therefore impossible to read all or at least the most important parts of the many privacy policies, which consumers have to accept for participating in the digital economy.[49]

(4) Consumers are also not aware of (and cannot assess) the value of their personal data that they provide to digital firms.

"Dark pattern" behavior

(5) A particularly important problem is that data-collecting firms can try to influence the decisions of the consumers with regard to consent with a broad range of instruments. In recent years a large literature about "dark pattern" has emerged that shows that through specific designs how the choice about consent (or opting-in or opting-out from certain purposes of data processing or sharing of personal data with other firms) is presented, digital firms can influence the decisions of the consumers. This is, in particular, based on behavioral insights into biases in the decision-making of consumers.[50] Especially wellknown is the default bias, i.e. that consumers tend to accept choices in pre-ticked boxes instead of opting-out again. However there are also many other ways how the choice architecture can be designed through buttons with

48 See also the discussions in Acquisti et al. (2016), Solove (2013), Bechmann (2014), Srinivasan (2019), Kemp (2020), and as overviews OECD (2020, 35-37), Kerber (2016, 644); see with respect to the "privacy paradox" also the overview in Kokolakis (2017). For a sector investigation of the problems of consumers regarding mobile apps see Federal Cartel Office (2021).

49 Specht-Riemenschneider/Bienemann (2019, 7 f.).

50 See e.g., Forbrukerradet (2018), Luguri/Strahilevitz (2021), Martini et al. (2021), Weinzierl (2020), Waldman (2020).

different colours, where the buttons are placed on the screen, making it more difficult not to consent (or opt-out again), using a confusing or misleading design, or setting the consumers under emotional or psychological pressure.[51]

In addition, digital platforms can easily experiment with different designs and test the response of their users, leading to much experience how they can influence the users (or different groups of users) to make decisions that do favour the interests of the data-collecting firms instead of the consumers. And with regard to the applied methods: "... online platforms are in an especially good position to maximize the impact of their choice architecture. ... this is due to the combination of three related factors: (i) extensive data about individual consumer behavior; (ii) machine learning algorithms that can mine these data for relevant behavioral patterns; and (iii) A/B testing techniques that are designed to industrialize trial and error experimentation to maximize the choice architecture's effect on users."[52] Due to these empirically well-confirmed new ways of informational and behavioral manipulation through "dark pattern" behavior, also a new discussion has emerged how to deal policy-wise with these new methods of influencing consumer decisions on digital markets.[53] Important for our discussion here is that especially the large digital firms, who have detailed consumer profiles about many users, and are the leading firms in data analytics, machine learning and algorithms, are in the best position to use these "dark pattern" behavior to influence the decisions of consumers with biased choice architectures with respect to the collection and use of personal data.[54]

Additional problems: Assessing privacy risks and "data externalities"

It is however necessary to take into account that also additional problems exist, which make it difficult that consumers can make the right decisions about the provision of their personal data:

(6) A particular difficult problem is that it is nearly impossible for consumers to assess the potential future privacy risks of allowing others to collect and use their personal data, especially if these data are also shared with a large number of other providers of services. This does not only refer to "data breaches" but also the manifold possibilities that these data, e.g. also by combining them with other data, are used for price discrimination, behavioral manipulation, the behavioral targeting of vulnerabilities, and misleading and fraudulent behavior.[55]

---

51 See an overview of different types in Martini et al. (2021, 52).

52 Digital Regulation Project (2021a, 18).

53 See, e.g., Martini et al. (2021), Digital Regulation Project (2021c, 17-24), and Luguri/Strahilevitz (2021, 82-102) for the discussion in the U.S.

54 See for dark pattern behavior also in later parts of the report, e.g., in sections 3.3.7, 3.4.2 and 3.4.3.

55 See Engeler (2021b, 4 f.).

(7) A very different and much more fundamental problem is the problem of "data externalities", which from an economic perspective is an additional market failure problem. Through the statistical analysis of large sets of personal data it is possible to infer much information about a specific person, if these data sets encompass many personal data from other persons with similar socio-economic characteristics. This implies that digital firms can know a lot about person A and her behavior, even if they do not have any personal data about this person. Therefore the revealing of personal data by other consumers can lead to negative ("externality") effects on the privacy of person A. Recent economic research has shown that such data externalities, which are presumably significant due to the abundance of collected personal data, can lead to a too low level of privacy, because denying the consent to provide personal data might not be a very effective instrument any more for protecting one's privacy.[56]

2.3.1.3 Conclusions

These manifold problems of the consumers to manage their personal data and protect their privacy lead to the danger that consumers increasingly come to the conclusion that their efforts for understanding privacy policies and trying to make informed decisions about giving their consent to the collection and use of personal data are futile and a waste of time.[57] If however many consumers either do not care any more, because they feel overwhelmed ("consent-fatigue"), or cannot assess easily the privacy-friendliness of different privacy policies of firms, then the conditions for an effective competition with privacy policies and privacy-friendly products and services are very difficult. We still would claim – based upon economic theory – that in a well-functioning market without these market failures competition would set incentives that firms offer privacy policies according to the privacy preferences of the consumers. Therefore policies, which try to solve the information and behavioral problems and help the consumers to make meaningful decisions about “their” personal data, might not only help directly informational self-determination and privacy protection, but might also help to enable effective competition with privacy policies.[58]

---

56 See Choi et al (2019) and Acemoglu et al (2021).

57 See Turow et al (2015), Condorelli/Padilla (2020, 181).

58 Even if competition with privacy policies can work, we should not expect however a clear correlation between the number of firms (firm concentration) and the positive effects on privacy. Such clear correlations also do not exist between the number of firms and other non-price parameters of competition, as, e.g. product quality or innovation. Therefore in cases of mergers, which would reduce the number of the firms, it would be necessary to investigate in a case-by-case analysis whether a merger has negative effects on privacy or not.

More transparency, e.g. also through standardisation and/or certification of privacy policies, privacy icons, as well as effective policies against misleading and manipulative practices (as "dark pattern" behavior) might help to make privacy policies more comparable and therefore allow consumers to identify better those privacy policies that fit better to their privacy preferences.[59] Consumer and data protection policy could therefore contribute to make competition with privacy policies more effective, which again would lead to positive (synergy) effects of competition on privacy. It is however not clear whether and to what extent it will be possible to solve these problems with the traditional (consumer) policy instruments, or whether also entirely new solutions as, e.g., new types of intermediaries (like PIMS: personal information management systems, and data trustee solutions) or new consent management systems might be necessary.[60] Overall, it is important to understand that the market for personal data suffers from serious market failures.

2.3.2 Effects of the level of data protection on the competitive advantages of the large digital firms

2.3.2.1 Introduction

In the discussion about the relationship between data protection law and competition law one of the most discussed topics refers to the question whether the EU data protection law with its high requirements for processing personal data (especially the need for opt-in consent) might lead to negative effects on competition. Particularly interesting is the question whether the GDPR strengthens the economic power of the large digital firms, because they might get – de facto – easier consent for collecting and use of personal data of consumers than other firms, and especially their European competitors.[61] If this thesis is true, then this would be one of the interaction effects from data protection law on competition, which might lead to a conflict between data protection law and competition. This might raise the question whether a lowering of the level of data protection in the EU might be a remedy for mitigating such negative effects on competition. However, due to the wellknown enforcement problems of the GDPR, it is also possible that the EU data protection law is only formally a very strict law but might have de facto a low standard of data protection due to severe underenforcement problems. We therefore will also ask the question whether there are other important reasons for competitive

59 See, e.g., Kettner et al. (2018), Efroni et al (2019).
60 See, e.g., Kettner et al. (2020).
61 See OECD (2020, 42).

advantages of large digital firms with respect to get easier consent than other firms for the collection and use of personal data. In this section we will analyze these questions and discuss possible policy implications.[62]

2.3.2.2 Studies about the effects of GDPR on competition

In OECD (2020) and Gal/Aviv (2021) comprehensive overviews about the existing literature and empirical studies can be found about the impact of the GDPR (and, more generally, privacy laws with opt-in consent) on different firm sizes, market concentration, competition and entry barriers. In the following, we summarize and critically assess the results of this literature:[63]

(1) There is a wide-spread agreement that the compliance costs of firms regarding the GDPR are significant and lead due to the existence of fixed compliance costs to a disproportionately higher burden for smaller firms than for larger and more diversified firms, and also to entry barriers for new firms.

(2) In a number of articles concerns were raised that privacy laws that require opt-in consent could lead to disadvantages for small and new businesses due to economies of scale and scope for getting consent, i.e. that larger and more diversified firms have relative advantages compared to smaller firms. The requirement of opt-in consent could therefore lead to a further entrenchment of the market position of incumbents, because they already have gotten consent in the past for collecting large amounts of personal data of consumers.[64]

(3) Another concern is that the requirements of the GDPR for processing personal data are also impeding the sharing of personal data between firms, because (a) the data can only be used for specific purposes to which the data subject has given consent, and (b) the data-sharing firm has – at least in some cases – also to take care of the compliance of the data-recipient. These impediments for data-sharing would favor larger conglomerate and vertically integrated firms. Since it makes it harder to get personal data from outside sources, it incentivizes more direct internal collection of data.[65]

---

62 These questions are also very relevant for the international discussion, because many countries view the GDPR as a model for their own new privacy laws.

63 See, e.g., Calgigo (2017), Campbell/Goldfarb/Tucker (2015), Matthew/Tucker (2019), Ohlhausen (2019), Gal/Aviv (2020). There are also a number of empirical studies that have tried to analyze whether the introduction of the GDPR has negative effects on competition, firm concentration, e.g. in online advertising, or third-party tracking. See, e.g., Libert/Graves/Nielsen (2018), Greif (2018), Moazed (2019), Johnson et al. (2021).

64 See Campbell/Goldfarb/Tucker (2015), Matthews/Tucker (2019), Ohlhausen (2019), and Gal/Aviv (2021, 353).

65 See, in particular, Gal/Aviv (2021, 353).

From all of these reasonings it can be concluded that the GDPR with its opt-in consent and strict rules how to use these data might lead to disadvantages for smaller and new firms and therefore have negative effects on competition. However, some of the authors of these studies as well as the OECD also emphasize that the larger control of consumers over “their” data through the GDPR can also have advantages, which might be larger than those possible negative effects on competition. However, it should be asked whether the objectives of the GDPR can also be achieved with less distortioning effects on competition.[66]

At first sight these reasonings about the effects of the GDPR and, especially, the opt-in consent are well-argued, and are partly also supported by empirical studies. However a deeper analysis leads to a much more mixed picture, especially also in respect to the policy conclusions that can be derived from this discussion. It certainly has to be acknowledged that compliance with the GDPR can cause considerable costs, and that larger firms have to bear a disproportionately lower burden with respect to these costs than smaller or new firms. It has however to be noted that nearly all regulations lead to relative advantages of larger firms compared to their smaller competitors, and it is not clear at all whether this is a bigger problem in the case of the GDPR than with other regulations.[67] There might also exist economies of scale and scope of larger and more diversified firms to get consent for personal data, but this will depend very much on the specific markets, on which these firms sell their products and services. Very important are, however, two other factors that might be responsible why especially the large digital firms might have advantages for getting easier consent, which are not addressed in this literature. The first factor refers to the already mentioned problem of a potential underenforcement of the GDPR vis-a-vis large digital firms, and the second factor might be the already existing entrenched market power and the lack of other options for the consumers. Both will be discussed in the next sections.

66 See OECD (2020, 43).

67 See, e.g., the large competitive advantages the large digital firms have regarding taxation in comparison with other less international firms.

2.3.2.3 GDPR: Underenforcement and legal uncertainty

An analysis of the enforcement of the GDPR shows that despite the fact that theoretically very high fines and other incisive measures exist to enforce the GDPR (Art. 58 and 85 GDPR), the data protection authorities of the member states of the EU, who have the task to enforce the GDPR, have so far been very reluctant in using their enforcement powers, especially with regard to the large digital firms.[68] Since the enforcement regime in the EU uses the "one-stop-shop principle" that stipulates that in principle only the data protection authority of that member state in which a firm has its main or single establishment has the authority to deal with all GDPR violations throughout the entire EU (Art. 56 (1) GDPR), the relevant data protection authorities for the large digital firms are the Data Protection Commission (DPC) in Ireland which is competent with regard to Google, Facebook, and Apple and the Commission Nationale pour la Protection des Données (CNPD) in Luxembourg which is competent for Amazon. Many observers and also other data protection officials have large concerns that the DPC is not doing enough to enforce the GDPR against these large digital firms, although there are large concerns about the compliance of these firms with the GDPR.[69] Only very recently has the DPC made its first decision against one of the large digital firms, after it was forced to amend its initially more lenient draft decision on the matter through the means of a binding decision by the European Data Protection Board (EPDS).[70] The CNPD has also recently issued its first decision regarding a considerable fine against Amazon Europe Core S.à.r.l.[71] There are concerns that the data protection authorities in these countries do not have incentives for a strict enforcement against these large digital firms that have chosen these countries as location for their headquarters.[72] It has, however, to be acknowledged that also the data protection

---

68 See the more detailed discussion in section 3.4.2.6; generally about the enforcement gap in data protection in Europe and the United States Lancieri (2021).

69 See e.g. the objections of eight data protection authorities to the DPC's draft decision on WhatsApp Ireland Ltd.'s data collection practices, as summarized in the EDPB's Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021. For a critical look at the DPC's enforcement actions, see also Thiel (2021, 469); Wagner/Ruhmann (2019).

70 EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021. The procedure necessary to arrive at such a binding decision is set out in more detail in section 3.4.2.6.

71 CNPD, Decision regarding Amazon Europe Core S.à.r.l., 6 August 2021, available at https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html, last accessed 22 September 2021.

72 Therefore the underenforcement vis-a-vis these large digital firms can be a consequence of jurisdictional competition for these large digital firms (forum shopping).

authorities in other member states are so far very reluctant in imposing high fines, which due to their deterrence function would give more incentives for full compliance with the GDPR.[73]

This underenforcement problem is also linked to the problem that with regard to many questions about the collection and use of personal data there is still large legal uncertainty about what practices and terms and conditions in privacy policies are allowed and which are infringing the GDPR.[74] Due to the reluctance of data protection authorities to initiate proceedings against potential infringements, the process of clarifying the rules of the GDPR through cases and decisions by the European courts has been so far very slow.[75] This combination of underenforcement and legal uncertainty about the correct interpretation of the data protection rules (with a broad range of interpretations in the legal literature)[76] has led to large grey areas and gaps, in which it is either legally not clear what the legal rules are and/or in which many practices, and presumably also entire business models, are de facto tolerated due to the lack of effective enforcement.[77] In such a situation, especially large digital firms have a wide scope for exploring practices with regard to the collection and use of personal data which might not only test the limits and exploit the loopholes of EU data protection law, but might also go far beyond what would be compatible with the GDPR. Due to their huge financial resources, the large digital firms do not have to fear high fines and can much better exploit these possibilities for the collection and use of personal data than other firms.[78]

In our overview about the potentially negative effects of the GDPR on competition it was claimed that large conglomerate and vertically integrated firms (as, e.g., the large digital firms)

---

73 For an overview over the fines imposed by the various national authorities, see table 1 in section 3.4.2.6.

74 See the more detailed discussion in section 3.4.2.2.

75 The CJEU e.g. has only had to decide on two cases concerning the GDPR from January to September 2021: CJEU's decisions on the GDPR from 2021: CJEU judgment of 15 June 2021 – Facebook/Gegevensbeschermingsautoriteit, C-645/19, EU:C:2021:483; CJEU judgment of 22 June 2021 – Latvijas Republikas Saeima, EU:C:2021:504.

76 One example is the discussion of what is "necessary for the performance of a contract" under Art. 6 (1) (b) GDPR, with e.g. Gierschmann (2022, 65) and Schulz (2018, 30) claiming that it suffices if the parties stipulate the data processing as the service contractually owed by the processor and e.g. Golland (2018, 131); Schulz (2018, 30) and Stemmer (2021, 41.1) arguing for an objective interpretation of the necessity criterion.

77 One example of this are "dark patterns" whose data protection implications are discussed in more detail in section 3.4.2.5 Data protection law could in theory counteract these patterns, but their use is not easy to prove in practice, Martini/Drews/Seeliger/Weinzierl (2021, 70).

78 However legal uncertainty and systematic underenforcement can also lead to another advantage for these large digital firms, because consumers tend to trust more well-known firms with strong brands than lesser known firms or unknown new firms, if it is not clear whether and to what extent firms comply with data protection rules and also ensure a high level of cybersecurity for avoiding data breaches. See for the advantages of the reputation of large firms in such situations of legal uncertainty Gal/Aviv (2021, 373).

have advantages regarding the use of collected personal data in comparison to smaller firms, because the GDPR erects multiple hurdles for the sharing of personal data with other firms or, vice versa, to get access to personal data from external sources. One particular problem is the purpose limitation of consent which requires to get new consent if these personal data are used for other purposes. In competition law there was always a "privilege" for large firms (that consist of many subsidiaries with own legal entities) because all behavior between these subsidiaries of this large firm was viewed as internal and therefore not subject to competition law ("Konzernprivileg").[79] However such a "privilege" for large firms does not exist in EU data protection law.[80] Data-sharing within a large firm consisting of different legal entities face the same rules for data-sharing as the data-sharing between different firms. Also the principle of purpose limitation applies in the same way. How can it be explained that these conglomerate firms can use much easier the collected personal data for different purposes in all parts of the firm? The solution is that the consumer has to consent to privacy policies of the large firm, which stipulate that all subsidiaries of the large firms and partner firms etc. can use these data in combination with a very broad description of the purposes of this data-processing. Therefore, these large conglomerate firms need only one consent for the sharing and use of these data within the entire firm.

However, from a data protection law perspective giving consent to such a wide sharing of data with such a broad consent regarding the purposes might often be not compatible with the GDPR.[81] It therefore can be claimed that if the rules about having to give consent to the use of personal data for specific purposes were to be properly enforced, then these conglomerate firms would not be so easily capable of using these data for manifold purposes in the entire firm. This implies that it is again the underenforcement of the GDPR which leads to these additional relative advantages of the large digital firms in comparison with their smaller or less diversified competitors. Therefore, it has been suggested, also from a competition perspective,

---

79 For the “Konzernprivileg” in competition law, see e.g. CJEU, Judgment of 24 October 1996 – *Viho*, C-73/95 P, ECLI:EU:C:1996:405, paras. 50 f.; Thomas (2020, 2, 693); more detailed: Thomas (2005, 236 ff.).

80 Bierekoven (2017, 284); Körner (2019, 1395); Spoerr (2021, 3a); Voigt (2017, 428); Wurzberger (2017, 259). However, some scholars argue that a “Konzernprivileg light” exists, as recital 48 GDPR states that controllers which are part of a group of undertakings may have a legitimate interest in transmitting personal data within a group of undertakings for internal administrative purposes, see e.g. Pfrang *(2019,* 161); Voigt (2017, 429); Wurzberger, (2017, 260).

81 Consent has to be given for “one or more specific purposes” (Art. 5(1)(a) GDPR). This criterion has to be interpreted narrowly, Albers/Veit (2021, 23).

that the data protection principle of purpose limitation should be used more as a solution for limiting the competitive advantages of the large digital firms.[82]

2.3.2.4 Market power on core platform markets

We think however, that the main reason for the competitive advantages of large digital firms with respect to getting the consent for the collection and use of personal data is their huge market power on their core platform services. Since most consumers have no realistic alternative options than using core platform services as the social media service of Facebook, the search engine or Youtube of Google, they are locked-in into the platforms and ecosystems of the large digital firms. The consumers are facing very often the situation, as it was claimed in the German Facebook case, that they have no genuine choice, and are therefore de facto "forced" to accept in a "take-it-or-leave-it" way the terms and conditions in the privacy policies of the large platform firms.[83] It is the huge market power and the de facto unavoidability of using the services of these large digital firms ("must-have" services) that makes it so easy for them to get not only the consent from the consumers, but also a very far-reaching consent about the collection and use of their personal data. On other markets, where consumers have a choice between different suppliers, it is much more difficult for the firms to get consent for the processing of so many data.

Refering again to our analytical framework, it is the competition market failure that in our view is the main reason for the huge competitive advantages of the large digital firms. This problem is aggravated by two additional strategies of these firms: The first one is the bundling of this consent with agreeing also to accept the merging of the personal data that are collected from other services and sources within or outside of the large digital firms, which increases tremendously the availability of personal data and how these data can be used, and lead to a further strengtheening of the competitive data advantage of the digital firms.[84] The second strategy is the building up of this far-reaching network of sources all over the internet, where the large digital firms (partly in exchange for services on websites or through their direct tracking activities) can collect personal data that they integrate into their consumer profiles.[85] It is very clear

---

82 See Caffarra/Ryan (2021). A stricter enforcement of purpose limitation might have similar effects as data separation remedies in competition law.

83 Condorelli/Padilla (2020, 181).

84 This is the strategy in the German Facebook case that was prohibited as abusive, also due to the exclusionary effects that are a result of the additional data advantages through this strategy. See about the anticompetitive effects of such a strategy of "tying of privacy policies" Condorelli/Padilla (2020, 181).

85 See ACCC (2019, 84).

that other firms outside of this small group of large digital firms do not have comparable possibilities to collect and use personal data.

2.3.2.5 Policy conclusions

Let us summarize our results: We have seen that there are well-argued and empirically plausible reasonings (compliance costs, economies of scale and scope) why the GDPR might lead to competitive advantages of larger and more diversified firms in comparison to smaller and new firms. We however claim that in respect to the small group of large digital firms it is primarily their economic power and their control over largely unavoidable core platform services that lead to the huge competitive advantages in comparison to their competitors with respect to their access to personal data. It is therefore the unsolved competition problem with respect to the large digital firms that is the main cause of the problem. Another important factor, which also has not been discussed enough in the literature about the effects of the GDPR on competition, are the effects of legal uncertainty and the serious problems of under-enforcement of the GDPR vis-a-vis the large digital firms.

What policy conclusions can be drawn from the results of this analysis? Since according to our analysis the main causes for the data advantages of the large digital firms are the huge market power of these firms and the underenforcement of the GDPR vis-a-vis these firms, the main policy conclusion is that these problems should be solved through competition policy and data protection law. Then it can be expected that these competitive advantages of the large digital firms would be reduced significantly (or even disappear). Lowering the standards of data protection law, e.g. by allowing more opt-out solutions regarding consent or extending the scope of other legal grounds for processing personal data, as, e.g., "legitimate interests" (Art. 6(1)f GDPR) would not be an appropriate policy response. Although such a strategy might make access to personal data easier for smaller companies, it is entirely unclear whether the large digital firms would not be capable to exploit these new options for collecting data much better than other firms. Although this would need much more research, it might well be that lowering the level of data protection and reducing the data subjects' rights might therefore lead to a further increase of the power of the large digital firms and their competitive advantages. Our conclusion is that instead the de facto standard of data protection should be increased through a more effective enforcement.[86]

---

86 This however also implies that a better solution of the market failure of information and behavioral problems is necessary, which also includes the solution of the problem of misleading and manipulative practices of firms ("dark patterns").

The decisive argument, however, is that EU data protection law has the task of protecting informational-self-determination of all natural persons (and therefore also consumers) as a fundamental value. This implies that consumers should have the right to decide about the use of "their" personal data, for enabling them to protect their privacy. This is part of the autonomy of individual persons, which is also important from an economic perspective as a precondition for a well-functioning market economy. Also from that perspective it is urgently necessary to solve the underenforcement problem of the GDPR. Therefore the benefits of this privacy regulation might be much larger than any remaining disadvantages for competition.[87] This, however, does not exclude that also efforts should be made to analyze whether it is possible to find ways how to reduce unnecessary hurdles for collecting and sharing of personal data according to the GDPR, e.g. for research purposes, without lowering the standard of data protection.

2.3.3 Data portability: Potential synergies with limits

A particularly important candidate for a powerful synergy effect between data protection law and competition law is the data portability right of Art. 20 GDPR: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided ...".[88] In the competition policy discussion this data portability right has been viewed as an instrument that might help to solve a number of competition problems that have emerged as new problems in the digital economy:[89]

(1) This right might be capable to foster competition between digital platforms (and ecosystems), because the option to port their data from one platform to another reduces switching costs of consumers and therefore mitigates their lock-in effects (and facilitates multi-homing). Therefore the data portability right might have a countervailing effect to the concentration tendencies of digital platforms.

(2) This data portability right can also help to solve the manifold competition problems that are caused by the lack of access to data. Often firms, and also the large digital firms, have exclusive control over valuable sets of data, and especially also personal data. Without access to

87 See also Gal/Aviv (2021, 387).
88 Art. 20(1) GDPR.
89 See, e.g., Crémer et al. (2019, 81-87), Graef (2020).

these data other firms might not be able to offer certain products and services to the consumers, i.e. they need access to these data for entering markets. With this data portability right the consumers can have “their” personal data ported from the data-holding firm to these service providers, leading to positive effects on competition, innovation, and consumer choice.

(3) Independent from the solution of specific competition problems, the data portability right can also be used by consumers to make their personal data more widely available to other firms for enabling data-driven innovation or scientific research.

Although from the perspective of EU data protection law the data portability right of Art. 20 GDPR is primarily seen as an instrument for informational self-determination, giving the data subjects more control over “their” data, it is also explicitly acknowledged in data protection law that it " ... is also an important tool that will support the free flow of personal data in the EU, ... foster competition between controllers .... and the development of new services in the context of the digital single market strategy."[90] In that respect fostering competition can be even seen as part of the objectives of EU data protection law. The problem however is that this data portability right has so far not fulfilled these expectations due to a number of severe problems with respect to its effectiveness. These problems have been analyzed and discussed in recent years, and triggered a policy discussion how this data portability right can be made more effective.[91] There are legal uncertainties, e.g. about the scope of the data portability right. Do the data that the data subject has "provided" also encompass "observed data", e.g. when data subjects use a smart device and the manufacturer of this device observes the behaviour of the data subject?[92] In addition, the data controller only needs to port the data, if this is "technically feasible", but there is no obligation for enabling technical feasibility. The use of this right by the data subject is also very cumbersome, and needs much time. In particular, no continuous or real-time portability is possible, which would be important for competition in various contexts. Additionally, also with respect to the data portability right an enforcement problem exists. The Commission has acknowledged these problems and has announced to consider also "mandating technical interfaces and machine-readable formats allowing data portability in real-time".[93] Without being able to discuss these proposals here in detail, we support measures for making this data portability right more effective, and enabling more data interoperability (e.g.,

---

90 Article 29 Data Protection working party (2016, 1).

91 For a comprehensive analysis and overview about the problems of the data portability right of Art. 20 GDPR and proposals for solving them, see Krämer et al. (2020, 75-84); see also Graef (2020).

92 See Article 29 Data Protection working party (2016, 9-10). This is however not clarified so far.

93 Communication of the European Commission: Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation. COM(2020) 264 final, 9.

through standardized APIs), as well as continuous and real-time portability can be very important in certain contexts.

Although the currently discussed proposals offer the chance that the data portability right is used more and also might help to a certain extent to foster competition, there are also inherent limits of the effectiveness of this right.[94] The main problem is that such a human rights-based data portability right as Art. 20 GDPR has to be applied in a similar way to all sectors and can encompass only personal data. However the competition and innovation problems that need to be solved through providing more access to data might differ considerably between different sectors and technological and economic contexts. This implies that the scope of data that is needed and the specific problems regarding its use might be very different, which would lead to the need of targeted solutions for the design of suitable data portability solutions. Since the data portability right of Art. 20 GDPR due to its human rights-based character cannot be adapted well to what is necessary to solve competition problems under different technological and economic conditions, it often will not be flexible enough for solving competition and innovation problems through a lack of access to data.

This is the reason why the data portability right for online bank account data was implemented by an additional sector-specific regulation, the Second Payment Services Directive (PSD2), in order to foster innovative financial services (Fintech).[95] Important is that this data portability right was specifically designed, and complemented with additional regulations about technical interfaces, security (e.g., double authentification) and fees (here: no fees) as well as the European Banking Authority as regulator. In order to achieve an effective solution, the legislator has not used the data portability right of Art. 20 GDPR, but instead enacted a separate, specifically designed sector-specific regulation. It can also be shown that the data portability right of Art. 20 GDPR is not capable of solving the data access problems with respect to the data of connected cars. Also here a sector-specific solution, e.g. through an additional reform of the type approval regulation for motor vehicles, which can be designed in a targeted way to the specific technological and economic conditions of the connected cars, offers a much better perspective for solving the competition problems, e.g. on the markets for repair and maintenance services.[96] Another approach to data portability rights was chosen with the concept of

---

[94] See for the following, Gill/Kerber (2020, 57-59); see also Graef (2020).

[95] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market [2015] OJ L 337/35. See also de la Mano/Padilla (2018).

[96] See for the problem of access to in-vehicle data in connected cars TRL (2017), Kerber (2018), Kerber/Gill (2019). The Commission has announced another reform of the type approval regulation for motor vehicles with the objective to solve competition problems through more access to the data of connected car (EU Commission 2020b, 28).

consumer data rights in Australia. In this approach consumers are granted rights on their consumer data, which however are not identical with personal data defined by privacy law. This should give the consumers more control over “their” (consumer) data as part of consumer policy (for consumer empowerment), and one of these rights is a data portability right with respect to these consumer data. Through this decoupling of the data portability right from privacy law, it can be much more flexibly designed, especially also to the specific needs of different sectors and their competition and innovation problems.[97]

In sum, the data portability right of Art. 20 GDPR can help to foster competition but – even after solving some of its current problems – it will only be helpful in a limited way, because it refers only to personal data and is - due to its human rights-based approach - not flexible enough for being well adaptable to the different needs for solving competition and innovation problems. Therefore it might be necessary (1) to define data portability rights, which are both broader and more targeted than the data portability right of Art. 20 GDPR, and (2) complement such data portability rights with additional regulations regarding security, technical interfaces (standardisation), and fees. One option is also to use data portability rights as specifically defined remedies in competition cases. In section 3.3.6 we will see that the proposal of the Digital Markets Act entails a far-reaching extended data portability right with mandated technical interfaces (APIs) and continuous real-time portability, both for the end users and the business users of core platform services of gatekeepers.[98]

2.3.4 Potential conflicts: Data access remedies in competition law and anticompetitive privacy strategies of large digital firms

In this section a number of issues will be addressed, where in the application of competition law potentially difficult (albeit limited) trade-offs might emerge, which however have to be dealt with also in a concrete way in competition cases. The first group refers to remedies in competition law, which intend to solve competition problems through obligations to give access to or share data with other firms, which however also might entail personal data. In section 2.3.3 we already have seen that lacking access to data can be an impediment for competition and innovation. For solving those competition problems, data access or data-sharing obligations can therefore be a remedy in competition law, i.e. that firms can claim access to data sets that are

97 See for the Australian consumer data right approach OECD (2020, 7-14) and Specht-Riemenschneider (2021, 430-436).

98 See Art. 6(1)h DMA and below in section 3.3.5.

held by other firms (e.g., according to Art. 102 TFEU or as part of remedies in merger cases). If these data sets are, however, encompassing also personal data, then such a competition law remedy can lead to a direct conflict with the privacy and the informational self-determination of the data subjects. Possible solutions are either that the data subjects have to consent to the sharing of their personal data with other firms, which however might lead to high costs, delays and the sharing of less data, or that data have to be anonymized, which however usually reduces the value and usability of the shared data for the data recipients. Both solutions lead to a diminished effectiveness of this remedy with respect to competition and innovation. Therefore we have a real trade-off between data protection and competition. There are some possibilities to mitigate this trade off, e.g., through advanced techniques of anonymization that lead to a lower loss of usability of the shared data. However, they will not be capable of eliminating entirely this conflict.[99] In section 3.3 we will see that some obligations in the DMA proposal, e.g. the sharing of search data with smaller search engine also have to face these problems of such a trade-off.[100] In our view, searching for suitable solutions for this trade off problem might be one of the important issues that should be addressed through collaboration between competition and data protection authorities.[101]

A second group entails cases, in which especially large digital firms like Google or Apple choose strategies that allegedly improve the privacy of consumers but simultaneously make it harder for competitors to get access to personal data, which can have exclusionary effects and hurt competition. Much discussed in the literature are (1) the plans of Google to phase out third-party tracking in its Chrome webbrowser and (2) the already implemented new app tracking policy of Apple.[102] In the latter case Apple obliges its app developers to give users the choice whether they want to be tracked by the app or not. This explicit opt-in solution to tracking has led to a dramatic reduction of the allowance rates for tracking after its introduction by Apple. Apple argues that such a measure increases the privacy of its customers. It is not possible here to analyze these cases in a deeper way. There are however large concerns in the literature that through such measures many firms are getting foreclosed from access to a vast

99 See Crémer et al. (2019, 104).

100 See below Art. 6(1)j DMA in section 3.3.7.

101 In the French GDF Suez merger case (2014), in which a competitor of GDF Suez requested access to its customer base, this conflict was solved by allowing the disclosure of these personal data (with the intention to protect competition) under the condition that the consumers could opt-out from the customer list of Suez GDF. It was however not necessary that all customers whose data were shared had to give consent. This compromise of an opt-out (instead of an opt-in) solution was the result of a consultation of the French competition authority with the French data protetion authority. See Crémer et al. (2019, 104) and BEUC (2018, 9). This implies that balancing these effects is possible but it is always a "delicate trade off" (BEUC 2018, 9). See also, more generally, about this problem Douglas (2020).

102 See, e.g., Geradin, D. et al. (2020), Sokol/Zhu (2021), Dnes (2021).

amount of personal data, which might have manifold negative effects on competition but also on the financing of the apps through the loss of revenue from targeted advertising. These and other cases, in which firms use privacy measures or insist on a particularly strong interpretation of EU data protection law (or other privacy laws) for arguing why they are not allowed to comply with requests for data access or data portability, raise a wide range of new questions about the relationship between competition law and data protection law,[103] which we cannot discuss here but which can be expected to get more relevant in the future.

Both groups of cases will play an important role in the future application of competition law , and – due to the key role of personal data on digital markets – also these trade-offs between remedying competition problems and the protection of informational self-determination will be important issues that also might lead to a direct conflict between competition authorities and data protection authorities. How to deal with these trade-offs? Important is that it is necessary to analyze these problems in a much deeper and differentiated way, because they might require very different and presumably also innovative solutions. As already indicated above, these potential conflicts might be most susceptible to be dealt with by a close collaboration of competition and data protection authorities.[104]

2.4 Intermediate results and two important policy conclusions

Summarizing some results

The task of chapter 2 was to provide a "mapping" of the relationship between competition law and data protection law, especially with respect to the economic power of the large digital firms. We have seen that the economic power of these firms is based both on their market power positions for core platform services that consumers can hardly avoid, and on the information power they are getting through their unprecedented access to data, especially personal data. From an economic perspective, it is the combination of two market failures, namely their market power, on the one hand, and information and behavioral problems of consumers, on the other hand, which does not allow the consumers to make voluntary, rational and informed decisions with regard to their personal data. This endangers their informational self-determination and consumer sovereignty, as well as their capabilities to protect their privacy. This combination of both market failures also leads to the deep intertwinement of competition law,

[103] One interesting question is whether privacy can also be used as a justification for alleged anticompetitive conduct. See Douglas (2021, 126 – 133).

[104] See below section 3.4.4.

data protection law and consumer law. This led to the insight of the need for an integrated approach, i.e. it is necessary to take into account the effects of both market failures and of the effects of all these policies for understanding how these digital markets work and what the role of the large digital firms and their economic power in the digital economy is.

The specific analyses of some important examples of potential synergies and conflicts between competition law and data protection law have shown that a too fast and superficial analysis might lead to wrong conclusions. The fact that so far competition with the parameter "privacy policies" has not worked well, does not imply that no positive (synergy) effects of competition on privacy exist, but can be explained by the simultaneous existence of the huge problems that consumers have to assess privacy policies and manage “their” personal data due to information problems and behavioral manipulation (dark patterns). Also the thesis that the alleged strict EU data protection law leads to significant competitive advantages for the large digital firms compared to other and smaller firms, might be misleading. We claim that it is the huge market power of these firms in combination with the systematic underenforcement of the GDPR vis-a vis these firms, which leads to significant advantages of the large digital firms with respect to the collection and use of personal data. The analysis of the competition-enhancing effects of the data portability right of Art. 20 GDPR has confirmed positive (synergy) effects of this right but also emphasized its limits, leading to recommendations for additional data portability solutions, e.g., as competition law remedies or additional (sector-)specific regulation. We have also seen that difficult conflicts between competition law and data protection law can arise in competition cases, if data-sharing remedies also entail personal data or large digital firms use privacy protection as an instrument for anticompetitive behavior.

Two general policy recommendations

For the following chapter 3 with its analysis of policies and proposals how to deal with the economic power of the large digital firms, we want to suggest two general policy conclusions that we think are particularly relevant:

1) Towards more asymmetric regulation of large digital firms: Stricter rules for competition, data protection, and consumer protection

In the competition policy discussion there is, in the meantime, already a broad consensus that the economic power of these large digital firms pose so large challenges that it is necessary to introduce additional rules for the behavior of this small group of firms. As we will see in sections 3.2 and 3.3, the current proposals or already enacted new provisions in Europe (EU: Digital Markets Act; UK: "pro-competition regime for digital markets"; Germany: Sect. 19a

GWB) are based upon the strategy that the current competition law with its ex-post control of abusive behavior is not sufficient, and therefore an additional layer of asymmetric regulation that targets primarily this small group of large digital firms is necessary.[105] The analysis of the economic power of the large digital firms in this chapter 2 supports this strategy for more asymmetric regulation of the large digital firms with respect to competition.

This analysis, however, also supports the policy recommendation that this policy strategy of more asymmetric regulation for the large digital firms should also be applied to data protection law and consumer law. The combination of market power (and having often de facto no choice) and information power (with its huge information asymmetries and potential for informational and behavioral manipulation) leads to much higher risks for informational self-determination, the protection of privacy, and consumer sovereignty than consumers have to face from other firms. Therefore subjecting these firms to stricter rules than other firms can be in a similar way justified and necessary as in competition policy. These stricter rules could focus on the market failure problems through information and behavioral problems (including behavioral manipulation), the protection of a minimum standard of choice for consumers, and also on a direct limitation of the collection and use of personal data through large digital firms for protecting the privacy of the consumers.

We are aware that both data protection law and consumer law are traditionally seen as horizontal regulations that should be equally applied to all sectors and to all firms. That means, for example, that in data protection law with respect to the collection and use of personal data the same rules should be applied to all firms, i.e. no differences are made between large and small firms. Therefore imposing stricter rules for this small group of large digital firms might seem to be incompatible with the current practice and jurisprudence of EU data protection law.[106] There are, however, two reasonings within data protection law that can, at first glance, be used to justify introducing stricter rules for these large digital firms also in data protection law. One refers to the risk-based approach of the GDPR, i.e. that if the data-collecting behavior of these firms leads to larger risks for the privacy of the consumers compared to other firms, then also a differentiation with respect to the allowed behavior can be justified. We will explain this later in this report.[107] The other reasoning refers to an "imbalance of power", which might lead to larger requirements with respect to consent for the large digital firms with their huge market

---

105 Please note that also the traditional control of abusive behavior of dominant firms is already an asymmetric regulation, because it implies additional rules for dominant firms that do not apply to non-dominant firms.

106 See Lynskey (2019, 203).

107 See 3.4.2.2.

power in comparison to firms that are under effective competition. In the legal literature these options for taking into account market power or data power have already been discussed at least to some extent, e.g. by proposing that firms with market power should have a "special responsibility" also in data protection law.[108] This implies that also the data protection law offers reasonings which might support the application of higher requirements (or stricter rules) for the collection and use of personal data for these large digital firms.[109]

2) Towards a more integrative and collaborative policy approach

Since on many digital markets the competition problems and data protection problems are not clearly separable any more, also due to the interaction effects between the existing market failures and between competition law and data protection law, the traditional approach of a strict separation of competition law and data protection law (and consumer law) is not sustainable any more. It is therefore necessary that each of these policies and legal regimes has to look also beyond their traditional boundaries, and also has to take into account the effects of the other market failures and the other policies on the digital markets, especially with respect to the problem of the huge economic power of the large digital firms. This requires a more integrative approach. It can also imply more collaboration between these policies and their enforcement agencies for solving the common problems, e.g. also through mitigating conflicts and achieving more synergy effects with respect to competition and data protection through the application of their legal instruments.

108 See Graef / Van Berlo (2020); see also Lynskey (2019) and Paal (2020).

109 In section 3.4.2 this will be analyzed in much more detail from a data protection law perspective, and also briefly in section 3.4.3 for consumer protection.

3. Policy solutions: Strategies, proposals, and perspectives

3.1 Introduction: Basic policy strategies

The second part of this report has the task to analyze how competition law, data protection law, and other related policies can be further developed for better dealing with the huge economic power of the large digital firms. In chapter 2 we already have seen that a particular important problem is the simultaneous existence of the two market failures, (1) competition problems, and (2) information and behavioral problems of consumers (inclusive "dark pattern" behavior), on digital markets for core platform services, where personal data play a key role. We have both an unsolved competition problem and an unsolved privacy and data protection problem, i.e. that consumers cannot sufficiently manage their personal data, which also endangers their consumer sovereignty. These problems are big challenges for competition policy and data protection (and consumer) law.

What policy strategies and specific policy proposals can be suggested for a more successful approach to deal with the power of the large digital (tech) firms in order to achieve simultaneously a better protection of competition and privacy (and informational self-determination)? How can conflicts between competition and data protection law be mitigated, enforcement gaps closed, and, in particular, synergies between both legal regimes more effectively used and strengthened? What additional policies and regulatory instruments can be used, further improved, and/or newly implemented that would complement competition policy and data protection law for strengthening both competition and data protection?

Basic strategy I: Integrating privacy concerns in the application of competition law

Since the decision of the German Federal Cartel Office (FCO) in the pioneer Facebook case in 2019, the question whether and how to integrate privacy concerns with respect to the large digital firms into the application of competition law is intensively discussed within the competition law community all over the world. Whereas traditionally competition and antitrust authorities (including the EU Commission) were very reluctant in taking into account privacy issues in competition cases, the most recent discussions in competition law have shown a remarkable shift to a much more open discussion with regard to consider privacy concerns in competition cases. Therefore, both competition authorities and competition scholars (lawyers and economists) have started to think about how to develop approaches, methods, and criteria how negative effects on privacy can be taken into account in the application of competition law, e.g. in

merger cases or abuse of dominance cases.[110] We will see below that also the "Digital Markets Act" proposal considers data protection aspects in its proposed obligations.

This basic strategy I is already a big step forward and asks primarily about how competition policy can take into account also privacy concerns. However, it does not focus directly on the interplay between competition law and data protection law. In this currently emerging competition law strategy with respect to privacy, competition scholars ask how they can apply or amend competition law given the currently existing data protection law, which has to be respected and might set strict limits, e.g. with respect to data-sharing remedies. Therefore, it is an unilateral approach of competition policy, which however starts to try to take privacy concerns seriously in the application of competition law. This is a huge progress and has to be welcomed.

Basic strategy II: Towards a more integrative and collaborative policy approach vis-a-vis the large digital firms

A second basic strategy would try to go much further into the direction of a more integrative and collaborative policy approach for dealing with the economic power of these large digital firms. It would analyze much deeper the interplay between competition law, data protection law, and consumer law, and ask what all of these different policies can contribute to solve these problems. It would try to develop a common strategy for dealing with these existing market failure problems (competition problems, and information and behavioral problems) on digital platform markets. It would ask how these policies can also help each other to achieve more effectively their objectives, and whether more coordination between these policies might offer the chance of more effective solutions for limiting the power of large digital firms, instead of uncoordinated applications of competition law, data protection law, and consumer law.[111]

Such an approach can be applied through a better bilateral alignment of the policies and more collaboration between enforcement authorities, as e.g., between competition law and data protection law. It can however also refer to a multilateral approach, which would include competition policy, data protection law, consumer law but also standardisation (and interoperability) policy, data policy (beyond data protection law), and also other new regulations. Such a more integrative and collaborative multi-policy strategy might offer entirely new and far-reaching

110 See as overviews OECD (2020) and Douglas (2021).

111 In the legal literature a more holistic approach has also been discussed for some time. See, e.g., Costa-Cabral/Lynskey (2017), Graef et al. (2018), Graef / Van Berlo (2020), Botta/Wiedemann (2020).

options for new policy strategies for limiting or even reducing the economic power of the large digital firms.

Structure of chapter 3

The policy discussion about the power of large digital firms is right now mostly focusing on approaches and proposals from a competition policy perspective. Both in Europe and the U.S. the challenges through the economic power of the large digital firms has triggered a far-reaching reform discussion in competition policy, which questions in a fundamental way the capability of the traditional competition (and antitrust) laws (and the current assessment concepts for their application) to deal successfully with this problem. Therefore, in Europe. far-reaching proposals of a more regulatory approach to the behavior of these large digital firms have been developed and are right now in the main focus of the discussion. This competition policy discussion will therefore also be in the main focus of our analysis in chapter 3.

In the next section 3.2 it will be briefly assessed whether and how the traditional competition law in the EU can deal with privacy concerns through competition problems, or whether more far-reaching solutions might be necessary. Whereas this discussion remains entirely within the basic strategy I, this is less clear with respect to the "Digital Markets Act" proposal of the EU Commission, although it is seen widely as closely related to competition policy. Due to its large differences to traditional competition law, the DMA proposal will be separately analyzed and discussed in section 3.3. Particular emphasis will be given to the question, to what extent and how the DMA also takes into account concerns about data protection and consumer policy, and how the DMA can be improved for achieving better competition, privacy, and consumer protection. This discussion will lead to proposals for the DMA that are related to the basic strategy II but also entail a more general assessment of the DMA and recommendations how to improve the current proposal.

The following section 3.4 will then ask – in line with basic strategy II – to what extent and how other policies, especially data protection law and consumer law, can contribute to solve the huge problem of the economic power of digital firms (sections 3.4.2 and 3.4.3). In these sections, it will also be asked whether these policies can also contribute to the strategy of more asymmetric regulation through imposing stricter rules on the large digital firms also with respect to data protection and consumer protection. The last section 3.4.4 will finally focus on the perspective of an integrative and collaborative approach between all these policies.

3.2 Solutions within competition policy

3.2.1 Introduction

After the large number of reports about the huge challenges of the large digital platforms, a broad opinion emerged in Europe in 2019/20 that traditional competition law might not be sufficient any more for dealing successfully with the power of the large digital firms. Particularly influential in that respect was the Furman report (March 2019), which explicitly made the argument that traditional ex-post competition law is too slow and ineffective, and therefore claimed the need for an additional pro-competitive ex-ante regulation of firms with a "strategic market status". A new regulatory unit (DMU: "digital markets unit") should have the authority to develop and enforce firm-specific "codes of conduct" for dealing with anticompetitive and unfair behavior of large digital firms vis-a-vis businesses and end users of these platforms.[112] The Furman proposal is so important, because all three new models that are currently discussed (or already enacted) in Europe can be seen as variants of the original Furman proposal:

(1) Although the new sect. 19a GWB is enacted within German competition law and is applied by the German competition authority, it is at least inspired by the Furman proposal, because it is targeting the same small group of large digital firms with new far-reaching quasi-regulatory powers of the Federal Cartel Office (FCO) their conduct vis-a-vis businesses and consumers.[113]

(2) The current policy proposals of the UK government about a new "pro-competition regime for digital markets" are directly based upon the Furman proposal.[114]

(3) Also the "Digital Markets Act" (DMA) proposal with its explicit introduction of an additional ex-ante regulation through a set of obligations for gatekeepers can be seen as a variant of the Furman proposal.[115]

Both the German, the UK, and the EU model have in common the assumption that an additional set of stricter rules for this small group of large digital firms is necessary that complements the (ineffective) traditional rules for the control of abusive behavior of dominant firms. Since however the approaches differ significantly, it is not surprising that an intense discussion

112 See Furman et al. (2019, 54-83)

113 See below section 3.2.3.

114 See CMA (2020b) and the consultation of the UK government (published: 20 July 2021): "A new pro-competition regime for digital markets", https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets.

115 See below section 3.3.

exists, which of the three approaches might be more effective.[116] In the broader (also international) competition policy debate it is also very controversially discussed, whether, on the one hand, such far-reaching reforms are necessary at all, and, on the other hand, not much more radical solutions, like, e.g. breaking up these large digital firms, might be necessary. In that respect the European proposals can also be interpreted as "moderate" solutions. Particularly important for our topic is, however, that - despite the awareness of the key role of personal data - privacy and data protection concerns do so far only play a very small role in this debate about far-reaching reforms in competition policy and the need and design of new ex-ante regulatory approaches for dealing better with the economic power of the large digital firms.[117]

In this section 3.2 we will not analyze again why additional stricter rules for the large digital firms are necessary, but ask, on the contrary, to what extent traditional competition law remains relevant, even if these new regulatory approaches are implemented, and whether and how it can take into account better privacy and data protection.

3.2.2 Traditional competition law

Does the introduction of specific ex-ante regulatory regimes for the large digital firms imply that traditional competition law is not needed any more for solving the problem of the economic power of these firms? All proposals have very clearly insisted on the principle that the new instruments should not preempt traditional competition law, especially also the ex-post control of abusive behavior of dominant firms (e.g., in the EU Art. 102 TFEU), and that both can be applied in parallel. Since these additional regulatory regimes (and also the German sect. 19a GWB) focus mainly on a limited set of unilateral anticompetitive and unfair behaviors, the application of traditional competition law remains the only option for dealing with a wide range of other behaviors of the large digital firms, like, e.g. anticompetitive agreements and, especially also mergers.[118]

It is therefore necessary to think also about reforms of the traditional competition law, e.g. with regard to procedural rules, rules about burden of proof, the causality principle, and judicial

---

116 See, e.g., Caffarra / Scott Morton (2021), Witt (2021b). We will come back to this question in section 3.3.8.

117 It is interesting, vice versa, that the new debate how to include more privacy concerns in competition law does not take into account these new regulatory approaches for taming the large digital firms (see, e.g., OECD 2020, and Douglas 2021).

118 It is one of the puzzling questions in this debate about a more regulatory approach in competition policy that all these proposals do not encompass new substantive rules for merger control, although the topic of the acquisition of new, fast growing digital firms through the large digital firms is acknowledged as one of the important problems. We will not discuss this aspect here in this report. See, e.g., Cabral (2021, 24-27).

reviews, which were seen as the main problems why the ex-post control of abusive behavior of dominant firms is viewed as too slow and ineffective.[119] This however might also entail changes of substantive competition law. For example, the 10th amendment of German competition law did not entail only the (below discussed) new sect. 19a GWB, but also introduced a broad range of other changes for strengthening the traditional control of abusive behavior (with respect to "market dominance" and "relative market power") for protecting competition in the digital economy (for example, with a specific focus on more data access but also procedural rules for facilitating data-sharing between firms).[120] For the future, it is therefore very important that policy-makers do not neglect traditional competition law, both at the national and the EU level. On the contrary, it is necessary to analyze deeper the current weaknesses and problems of traditional competition law and develop solutions for making it more effective.

In the following, we will focus on the more specific question how traditional competition law is dealing with privacy and data protection concerns, and what proposals can be made for strengthening synergies and avoiding conflicts. The very controversial discussion about the German Facebook case has shown that in Germany, the EU, and also internationally the traditional approach in competition law is still dominated by the "separation thesis", i.e. that competition law should deal with competition problems, and privacy problems should be solved by data protection law.[121] In the meantime, it has been understood and accepted that privacy can also be seen in competition law as part of quality (as a non-price parameter) and that privacy harm might be interpreted as consumer harm, which would allow its consideration in competition cases.[122] However, the current practice, also in EU competition law, has shown that privacy concerns do only play a very small role in competition cases, e.g., in merger cases. In particular, the EU Commission has been very sceptical about including privacy concerns in competition cases.[123] This is partly a consequence of the traditional over-emphasis on prices and neglect of the non-price dimensions of competition. Very important, however, is also the lack of research about theories of harm with respect to privacy harms (and also how to measure privacy risks and harms). Another problem is that interaction effects between data

119 See, e.g., Crémer et al. (2019, 41-51).

120 Therefore the reform of the German competition law has a two-pronged approach: Introducing the new sect. 19a GWB as a special provision targeting the large digital firms, and, in addition, also changing a number of other substantive and procedural rules for making competition law more effective on digital markets, also with respect to the large digital firms. See for a broad overview about the reform of German competition law Käseberg et al. (2021).

121 See e.g. Körber (2019), Buiten (2020), the Facebook decision of the OLG Düsseldorf (2019; rejecting the decision of the FCO), and for the US, e.g., Ohlhausen/Okuliar (2015), United States (2020). See for the separation thesis also above section 2.2.

122 See Douglas (2021, 62-74).

123 See OECD (2020, 26-29); see also Robertson (2020, 187).

protection law and competition are not taken into account properly, e.g. that the EU Commission erroneously assumed in competition cases that EU data protection law would be properly enforced and effective, e.g. with respect to the data portability right of Art. 20 GDPR.[124]

The Facebook case of the German Federal Cartel Office (FCO) was a "game-changer" in that respect, and triggered a broad and international discussion about the role of privacy in competition law, and the general relationship between competition law and data protection (or privacy) law. It was the first case, in which a competition authority has prohibited certain terms and conditions about the collection and use of personal data as an abusive behavior of a dominant firm.[125] As already briefly described in section 2.1, the abusive behavior refers to the requirement of Facebook in its privacy policy that users of its social media service have to give also consent to the merging of all personal data that Facebook collects about them through other services of Facebook and also third-party websites in one Facebook account (leading to comprehensive consumer profiles). The FCO argued that due to the dominant position of Facebook on the German market for social media services the users are "forced" to give their consent for this combination of collected data. In its decision the FCO imposed the remedy that the users should have an additional choice to consent or not consent to the merging of these data into one data set. It was particularly interesting from a competition law perspective that the FCO framed the decision primarily as an exploitative abuse (with also exclusionary effects), and used the argument that these terms and conditions violated EU data protection law as criterion for the abusive character of this behavior.[126] This use of data protection law in a competition case was unprecedented, and also provoked the allegation that the FCO uses competition law for enforcing data protection law.[127]

Although the legal proceedings in this case are ongoing and a final decision still seems far away, the impact of this case are already far-reaching. Not only did it lead (1) to the international discussion about whether and how to consider privacy in competition law, it also led (2) to the inclusion of this Facebook remedy (of an additional consent for combining personal data) as a general obligation in the DMA.[128] More generally speaking, it (3) suggested the new idea of introducing a minimum standard of choice for the data subjects in competition law with respect to their decisions about how their personal data are collected and used. Already the FCO emphasized the importance of having a genuine choice vis-a-vis a dominant firm, and not

124 See OECD (2020, 29).
125 See Federal Cartel Office (2019).
126 See Robertson (2020).
127 See Colangelo/Maggiolino (2019, 376).
128 See below section 3.3.

having to accept any take-it-or-leave-it conditions about “their” personal data. Particularly important was, however, the decision of the German Federal Court of Justice in the interim proceedings about the Facebook case, which claimed that not giving this choice would violate the "basic value" of informational self-determination in the German constitution, which grants the German citizens the right to substantially participate whether and how their personal data are collected and used by others.[129] These reasonings are important, because they do not focus primarily on excessive data collection in analogy to excessive prices, but emphasize directly the extent of choice that consumers and data subjects have. These decisions of the German FCO and the Federal Court of Justice therefore suggest that competition law can also be used for ensuring a minimum standard of choice, especially with respect to the collection and use of personal data (informational self-determination).[130] We will come back to this reasoning in our discussion about Art. 5(a) DMA.[131]

It is however unclear what the implications are for traditional competition law. The Facebook case is still far away from a final decision.[132] Since the entire case is based upon German competition law, it is not clear, whether this behavior would also be seen as abusive according to Art. 102 TFEU in EU competition law.[133] Since privacy is a fundamental value in the EU, the same reasoning of protecting a minimum of freedom of choice vis-a-vis dominant firms should also be applicable at the EU level. A crucial question, however, is whether and to what extent the EU Commission is willing to change its so far very reluctant policy about taking into account privacy concerns in the application of traditional competition law.[134] It can also be asked whether the inclusion of this Facebook remedy (additional consent for combining personal data) as a general obligation for gatekeepers in Art. 5(a) of the DMA proposal might be a signal that, in the future, the EU Commission will take privacy and data protection concerns more into account also in traditional competition law, e.g., with respect to abusive data-collecting behavior of dominant firms like Facebook or Google. All of these questions are right now open questions.

---

129 See Federal Court of Justice (2020, 47-49); see for this decision Podszun (2020).

130 See for this decision and its link to autonomy and a minimum standard of choice Podszun (2020), Wiedemann (2021), and Kerber/Zolna (2021, 22-25).

131 See below in section 3.3.4.

132 After the interim decision of the German Federal Court of Justice, the OLG Düsseldorf has made in March 2021 a reference for a preliminary ruling for clarifying legal questions to the Europan Court of Justice (OLG Düsseldorf 2021).

133 This is supported by Volmar/Helmdach (2018), Schneider (2018), and Robertson (2020).

134 The current controversial discussion about the recent decision of the EU Commission in the Google/Fitbit merger case reflects this problem. See EU Commission (2020c), Bourreau et al. (2020), BEUC (2020).

What recommendations can be made about taking negative effects on privacy and data protection better into account in competition law?[135] Particular important is that more research is necessary about how competition problems can lead to negative effects on privacy and informational self-determination, especially also with respect to potential harms of data-collection and data-combination. This also is directly linked to the issue of developing better concepts and methods for analyzing these questions in competition cases.[136] As competition scholars had to develop assessment concepts for price effects in the past, this is also necessary in a similar way for privacy effects. Such research should also focus on the analysis of exclusionary effects of privacy-harming data collection practices.[137] This is a task mainly for academic research and competition authorities, which, however, might also require a close collaboration with the privacy and data protection scholars and data protection authorities. If traditional competition law does not turn out to be flexible enough for taking better into account also privacy concerns, then it also can be thought about including privacy and data protection as an explicit additional objective in the competition law.[138] It should, however, also be seen that the possibilities of traditional competition law will always remain limited with respect to solving privacy and data protection problems, because competition law cannot deal in a systematic way with the market failure of information and behavioral problems, which, as we have seen in chapter 2, is another crucial problem that has to be solved with respect to the economic power of the large digital firms. We will come back to this problem in section 3.4.4 as part of our discussion about the need for a more integrative and collaborative policy approach.

3.2.3 The new Sect. 19a GWB in German competition law

In its 10th amendment of German competition law (enacted in January 2021) Germany was the first country that has introduced with the new sect. 19a GWB a new additional set of behavioral rules that are intended to target the economic power of the large digital firms. In contrast to the Furman proposal and the DMA at the EU level, this additional layer of behavioral rules is included directly in German competition law and will be applied by the German competition

---

135 See for broad and comprehensive reviews to what extent and how competition law already tries to take into account privacy effects in competition cases, and which problems arise in that respect in competition law, OECD (2020, 24-40) and Douglas (2021, 62-144). Such an analysis could not be done in this report.

136 See the recommendations in Douglas (2021, 144-147)

137 See for the discussion about the need for new theories of harm and methods Douglas (2021, 144-147). For supporting this basic research, the EU Commission and the member state governments could, e.g., provide research grants.

138 This would be particularly possible in national competition laws. Another hurdle for taking into account abusive data-collecting behavior of dominant firms, namely the problem of "conduct causality" ("Verhaltenskausalität") has already been solved by the German legislator in the 10th amendment of German competition law.

authority.[139] There are no doubts that these rules are legally part of competition law, and exist additionally to the traditional ex-post control of abusive behavior of dominant firms (sect. 19 GWB), which also remains applicable to the large digital firms. Particularly innovative is the concept for defining, for which firms these additional rules can apply. The approach to focus on firms with a "paramount significance for competition across markets" emphasizes the conglomerate character of the large digital firms with their platforms and ecosystems and manifold cross-market effects.[140] This goes far beyond market power on traditionally defined markets, and therefore can encompass much more aspects of economic power than traditional concepts of market dominance, which always have to focus on specifically defined markets. This also implies that in the list of criteria that can be used for assessing whether a firm has "paramount significance for competition across markets", market dominance on specific markets is only one criterion under others, and it is not necessary that such a firm is dominant on any market.[141] In a first step, the German competition authority has to make a decision, whether a firm has this status of "paramount significance for competition across markets", before, in a second step, it can prohibit certain behaviors of these firms. It is no particular problem to address with this provision the large digital firms and also their gatekeeper positions on their digital platforms.

If a firm is designated as having such a status, the German competition authority can prohibit a wide range of behaviors as e.g. self-preferencing, hindering supply or sales activities of other firms, using collected data for raising entry barriers, impeding interoperability or portability of data, or not giving business users access to information about their performance.[142] These behaviors are to a large extent overlapping with the obligations in the DMA proposal but the behaviors that can be addressed are much more openly described, and will partly also go beyond what will be prohibited according to the current DMA proposal. Important however is that these behaviors are not directly prohibited (as in the DMA proposal), they rather offer the German competition authority a menu of options which behaviors they can prohibit. Since it is the intention of this amendment to have a faster and more effective enforcement, sect. 19a GWB introduces a shift of burden of proof, i.e. there is a strong presumption that such behaviors of this group of firms will lead to impediments of competition, but the firms have the

---

139 Bundesgesetzblatt (Federal Law Gazette), 18 January 2021, Part I No. 1, 2 et seq. Available at *https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27%27%5D#__bgbl__%2F%2 F*%5B%40attr_id%3D%27bgbl121001.pdf%27%5D__1611317574622.* For the sect. 19a GWB see Lettl (2021), Franck/Peitz (2021), and Witt (2021b).

140 Sect. 19a (1) GWB.

141 See Franck/Peitz (2021, 4).

142 See sect. 19a (2) sentence 1, No. 1 – 7 GWB.

possibility of justifications. Through this presumption and the shift of "burden of proof" sect. 19a GWB seems to get somehow also the character of a quasi ex-ante regulatory approach, but since these rules cannot be seen as per-se prohibitions[143] and due to the explicit option for justifications of the firms, it is an open question how effective this new instrument will turn out, if the cases go to the court.[144]

Overall, the new sect. 19a GWB offers an innovative and particularly flexible instrument for the German competition authority to address a wide range of potentially abusive behaviors of the large digital firms, and can therefore help to deal with the economic power of the large digital firms.[145] It might also be a valuable complementary instrument after the enactment of the DMA at the EU level. Since it is, however, part of competition law, it will not be easy to take into account also data protection and consumer policy concerns. However, some of the seven groups of behaviors, which can be prohibited by the German competition authority, also refer to the interests of consumers and data subjects with respect to their personal data. This is relevant, primarily, for sect. 19a (2) No. 2, 3, 4, and 5 GWB, which focus on different aspects of protecting choice for the users (including interoperability and data portability). Especially the provision of No. 4a, which protects freedom of choice ("Wahlfreiheiten") of users with respect to consent regarding the processing of personal data, is very close to the obligation of Art. 5(a) in the DMA proposal (and therefore the remedies in the German Facebook case). It is not possible to discuss these German provisions here in a deeper way. However, many questions that are discussed below with regard to Art. 5(a) DMA proposal might also be similarly relevant for this German provision.[146]

---

143 See Franck/Peitz (2021, 8).

144 See for many open question in that respect Witt (2021b). It is especially unclear to what extent it is necessary to balance pro- and anticompetitive effects (see also Franck/Peitz 2021, 10). Important for the fastness of legal proceedings is that the sect. 19a decisions are subject to an abridged judicial review, because they go directly to the Federal Court of Justice. See Franck/Peitz (2021, 13) who see this also critically.

145 In 2021, the German FCO has already initiated several new investigations against Facebook, Amazon, Google, and Apple using this new provision of sect. 19a GWB. See, e.g., Facebook/Oculus - https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html?nn=3591568

146 See below section 3.3.4.

3.3 The "Digital Markets Act" Proposal

3.3.1 Introduction and overview

For the EU Commission the proposed "Digital Markets Act" (DMA)[147] as a new ex-ante regulatory regime would be the key instrument for dealing with the economic power of the large digital firms. In contrast to the Furman proposal and the new sect. 19a GWB in Germany, the DMA does not address directly the large digital firms but focusses instead on the regulation of gatekeepers on markets for core platform services, which have to comply with overall 18 behavioral obligations. Since the main problems of traditional ex-post control of dominant firms are seen in too lengthy proceedings, problems of providing evidence, and ineffective remedies, the basic regulatory strategy of the DMA is that gatekeepers have to comply directly with these obligations, without the need for investigations, proving of harm, and decisions of the Commission (as they are, e.g., necessary in the German solution and in the Furman proposal). This offers the chance of a much faster enforcement of these obligations. The obligations themselves cover a broad range of behaviors, which are seen in the discussion about platforms as potentially problematic behavior of large digital platforms, and are derived mostly from past and current competition cases.[148] The DMA proposal is currently discussed in the European Parliament and the Council, and it is expected that a final version of the DMA might be enacted early next year.[149]

Since the DMA is the most important current legislative project for the topic of this report, section 3.3 will assess the DMA proposal more deeply. In addition to the question whether the DMA can be an effective instrument for limiting the power of the large digital firms and strengthen competition, it will also be analyzed regarding its contribution to data protection and consumer policy objectives. Since the DMA has so far been mostly discussed as a competition-oriented ex-ante regulation, this section wants to complement (and perhaps "debias") this discussion by offering an additional analysis from a data protection and consumer policy perspective.[150]

---

147 Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

148 See generally about the DMA, e.g., Caffarra / Scott Morton (2021), Cabral et al. (2021), de Streel (2021a, 2021b), Ibánez Colomo (2021), Kerber (2021c), Monti (2021), Podszun/Bongartz/Langenstein (2021), Schweitzer (2021), Zimmer/Ghösl (2021), Larouche/de Streel (2021).

149 See, e.g., the draft opinions of the IMCO committee, the JURI committee, and the ECON committee of the European Parliament, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0374(COD)

150 For position papers from a data protection and consumer policy perspective, see EDPS (2021), BEUC (2021), and vzbv (2021).

The analysis is structured as follows. After a brief analysis of the general approach of the DMA (section 3.3.2), the objectives and the per-se rules vs. flexibility issue as two of the most controversially discussed problems of the DMA will be discussed (section 3.3.3). This will be followed by a deeper investigation into several obligations (section 3.3.4 to 3.3.7), which are particularly relevant for data protection and the interests of consumers. In this part we also will make recommendations regarding the amendments of these obligations including the proposal of an additional obligation. The final section 3.3.8 will offer a brief overall assessment of the DMA with further recommendations for improving its effectiveness. Based upon our recommendation in chapter 2 to apply more asymmetric regulation on the large digital firms also for data protection and consumer protection, we will analyze also the perspective to view the DMA not only as an asymmetric regulation instrument for competition but also for data protection and consumer protection.

3.3.2 General approach

The problems that the DMA wants to address are, on the one hand, the contestability of the large digital platforms, which enjoy entrenched and durable positions (due to large network effects and conglomerate ecosystems), and, on the other hand, unfair behavior of the platforms vis-a-vis business and end users. This unfair behavior is possible through the fact that these platforms act as gatekeepers for the intermediation of business and end users, leading to the dependency of these users on the platform. These unfair practices and lack of contestability does not only have negative effects on the business users but also leads to "higher prices, lower quality, as well as less choice and innovation to the detriment of European consumers".[151] "The objective of the proposal is therefore to allow platforms to **unlock their full potential** by addressing at EU level the most salient incidences of unfair practices and weak contestability so as to allow end users and business users alike to **reap the full benefits of the platform economy** and the digital economy at large, in a contestable and fair environment."[152] The objectives of the DMA are therefore "contestability" and "fairness", which, as we will discuss below in more detail, are controversially discussed but are supposed to be significantly different from the objectives of traditional competition law with its assessment criterion of the effects on consumer welfare.

Also the architecture of the DMA differs significantly from traditional competition law. It is an ex-ante regulation, which establishes with its 18 obligations a per-se rule regime for

151 DMA, 1.
152 DMA, 2 (emphasis in the text).

gatekeepers as providers of core platform services. The scope of the DMA is defined, on the one hand, through a closed list of eight core platform services, as, e.g., online intermediation services (e.g., Amazon market place), online search engines (e.g., Google search engine), online social networking services (e.g. Facebook social media), and video sharing platform services.[153] However, only very large providers of such services raise serious concerns regarding the objectives contestability and fairness, leading to their designation as gatekeepers, who then have to comply with these obligations for their core platform services. Three criteria have to be fulfilled: They should have (1) significant impact on the internal market, (2) operate one or more important gateways to consumers, and (3) enjoy (or are expected to enjoy) an entrenched and durable position. For facilitating the designation of gatekeepers by the Commission the DMA use concrete quantitative thresholds, e.g. with respect to turnover, the number of business and end users etc., whose fulfillment lead to a strong presumption that such a provider is a gatekeeper.[154] The DMA also differs significantly from traditional competition law, because the designation of gatekeepers does not require the definition of markets or an assessment of market dominance.

These gatekeepers have to comply directly with all 18 obligations with respect to their core platform services. The DMA distinguishes between Art. 5 obligations and Art. 6 obligations. Whereas the Art. 6 obligations might need further specification, the Art. 5 obligations are supposed to be clearly specified enough for direct compliance by the gatekeepers. As far as further specification is needed, the DMA offers a procedural framework that also includes the possibility of a regulatory dialogue between the Commission and the gatekeepers, and also allows the Commission to make decisions about further specification.[155] For being capable to deal with the dynamics of the digital markets, an update mechanism with respect to the list of core platform services and the list of obligations plays a key role in the architecture of the DMA.[156] The complex process of enforcing the DMA cannot be described here, but in the discussion about the DMA a number of proposals were made for strengthening its enforcement.[157]

---

153 Additional core platform services are number-independent interpersonal electronic communication services, operating systems, cloud computing services, and advertising services (Art. 2(2) DMA). In the discussion about the DMA proposals have emerged for extending this list, e.g., by smart virtual assistants (vzbv, 2021, 7).

154 Art. 3 DMA. However this presumption can be rebutted by the firms as well as the Commission can also designate a firm as a gatekeeper after a market investigation, if these quantitative thresholds are not fulfilled. For critical analyses of the designation of gatekepers, see Geradin (2021), de Streel et al. (2021b, 9-19), Monopolkommission (2021).

155 See Art. 7 DMA.

156 See Art. 10 and Art. 17 DMA (based upon a market investigation).

157 See below section 3.3.8.

3.3.3 Objectives and flexibility: Two controversially discussed problems

3.3.3.1 The objectives "contestability" and "fairness"

A particularly interesting and so far controversially discussed question refers to the interpretation of the two objectives of the DMA, namely "contestability" and "fairness", especially in combination with the explicit statement in recital 10 that the DMA protects different legal interests than traditional competition law (in Art. 101 and 102 TFEU), and should therefore not be seen as part of competition law. Although "contestability" refers in economics to the question how easy it is for other firms to enter a market and challenge incumbent firms and is therefore about keeping markets open and competitive, this objective is different from what is done in the current assessment in traditional competition law, which focuses mainly on the question whether a behavior has negative effects on consumer welfare.[158] It is clear that fairness is a much more difficult objective, because it can be understood very differently. In competition law there was always much reluctance in using the concept of fairness as assessment criterion. It is one of the interesting characteristics of the recent reform discussion in competition policy that the concept of fairness plays a much more prominent role.[159] However "fairness" is an open concept that not only can be interpreted differently but also might encompass several distinct dimensions.

How can "fairness" be understood? The DMA sees a direct link between the gatekeeper position, and the ensueing "serious imbalances in bargaining power", which lead to "unfair practices and conditions for business users as well as end users of core platform services ... to the detriment of prices, quality, choice, and innovation therein".[160] Especially with respect to the business users this leads to "an imbalance of rights and obligations on business users and the gatekeeper is obtaining an advantage from business users that is disproportionate to the service provided by the gatekeeper to business users".[161] It seems that this approach focusses on a distributional question between platforms and business users, i.e. a fair sharing of the value that is created ("sharing of the surplus"). In the debate about the DMA also much broader notions of fairness have been suggested.[162]

---

158 For an excellent discussion of "contestability" (and its economic background) and how it could be interpreted in the DMA from an economic perspective, see Digital Regulation Project (2021c, 14-25).

159 See, e.g., the Furman report, where the term "unfair" behavior was widely used (e.g., Furman 2019, 46).

160 Recital (4) DMA.

161 Art. 10 (2) DMA.

162 In the following, we rely mainly on the discussions in de Streel (2021b, 42-49), Podszun et al. (2021), and Digital Regulation Project (2021c, 6-14). For additional discussions see, e.g., Schweitzer (2021), Cabral et al. (2021, 30-32).

Based upon this discussion we summarize our position with regard to the interpretation of this objective "fairness" and how it can be used in the DMA:
(1) Since the end users (usually consumers) are in a similar way, or often even more, dependent on the core platform services of the gatekeepers, it is important that the consumers are also protected against the negative effects of the economic power of the gatekeepers. The text of the DMA is unclear and inconsistent with respect to the question whether primarily business users should be protected or also end users. In our view both groups of users should be protected by the DMA, and the text of the DMA should be clarified in that respect.[163]
(2) Unfair practices through the economic power of the gatekeepers can work in different ways and lead to different kinds of negative effects:
(a) One effect is about an unfair sharing of surplus, which, e.g., can also consist of the problem that business and end users cannot "reap the just rewards for their contributions to economic and social welfare".[164] This is also related to the basic idea of "exploitative abuse" through firms with market power in traditional competition law.[165]
(b) Another dimension can refer to the autonomy of the business and end users, i.e. that business users are not unduly restricted in their freedom to compete, and that consumers have enough choice for making their own decisions about their consumption and whether and how their personal data are collected and used.[166]
(c) However, fairness can also refer to transparency and being protected against misleading practices and dark pattern behavior for influencing end users, e.g. through biased choice architectures or biased rankings and ratings.[167]

Very important from our perspective is that this fairness concept can deal (1) with both market failures, i.e. imbalances of power and information and behavioral problems. (2) It implies for business users that they are protected against intransparent and unfair rules on platforms, undue restrictions of their ability to compete with their own business strategies, and not being deprived of the rewards for their performance and innovations. This also can be called the

163 See also BEUC (2021, 5-7), vzbv (2021, 4). Digital Regulation Project (2021c, 7); also de Streel et al. (2021b, 45) are discussing this question but then decide to stick to a narrow definition of fairness, which only protects the "commercial opportunities" of business users.
164 See Digital Regulation Project (2021c, 6).
165 See also Schweitzer (2021), who emphasizes the close connection of fairness with exploitative abuse.
166 See Podszun et al. (2021, 62), Marsden/Podszun (2020, 46), who call this "independence of decision-making". It is also directly related to "consumer sovereignty".
167 See also Digital Regulation Project (2021c, 11-13), where also additional dimensions of fairness are distinguished, as "fairness of contractual terms" and "fairness in process and practices". For Podszun et al. (2021) this can be seen as part of "fairness in intermediation".

protection of "commercial opportunities" of business users.[168] This protection of the freedom and ability of business users to compete is a key precondition for a well-functioning market economy. (3) With regard to the consumers and end users it allows to take into account also the objectives of data protection and consumer law, i.e., informational self-determination / consumer sovereignty with its dimensions of (a) strengthening autonomy (and ensuring choice), and (b) protecting against informational and behavioral manipulation (information power).

As a consequence, it is no problem that the DMA can also take into account the objective of data protection law and consumer policy. On the contrary, the result of our chapter 2 has shown that it is also the combination of both market failures that leads to the huge economic power of the large digital firms. Therefore, it is also consequent that the DMA, which has the task of dealing with the power of these firms, should not only be seen as a new ex-ante version of a competition policy instrument but as a regulatory instrument that also takes into account data protection and consumer policy objectives. It would therefore fit to our claim for more asymmetric regulation of the large digital firms with respect to competition, data protection and consumer protection (section 2.4). The concept of fairness is not only flexible enough for enabling such an approach, we even will see in the following analyses of the obligations that such an interpretation would lead to a more consistent approach in the DMA.

168 De Streel (2021b, 44) use this term "fairness of commercial opportunities" but define it in a more narrow way, because their definition encompasses the first two aspects but not the aspect of a fair sharing of surplus.

3.3.3.2 Per-se rules vs. flexibility / differentiation

Very controversially discussed is also the question whether this ex-ante regime of a fixed set of obligations, with which all gatekeepers have to comply, is too rigid and inflexible. Already the first commentators made the important point that the business models of these gatekeepers are very different, which implies that the effects of the same behavior on contestability and the capability and incentives for unfair practices might differ significantly between the gatekeepers. Therefore, different gatekeepers with different business models might need different obligations, and not a one-size-fits-all solution.[169] Others made the argument that the gatekeepers should also have the option of an efficiency defence, which is not possible according to the DMA proposal.[170] Also other justifications, e.g. that the gatekeepers can show that their behavior (despite not complying with the obligation) does not lead to less contestability and more unfair practives, are excluded in the current proposal, and therefore demanded by some commentators.[171] Whereas these flexibilities would give gatekeepers options for defending themselves, other commentators claim, vice versa, that such a rigid set of obligations can also be hindering an effective enforcement, and it should be therefore possible that the Commission can also impose additional gatekeeper-specific obligations for better protecting contestability and fairness.[172]

From an economic perspective it is clear that a per-se rule regime that applies all obligations to all gatekeepers with their core platform services will certainly lead also to wrong decisions. However, the approach in the ex-post control regime of Art. 102 TFEU, in which the Commission has to prove in each case the anticompetitive effects, has not worked either in the digital economy, and led to a huge underenforcement of competition law. Therefore, accepting a limited number of erroneous prohibitions (type I errors) might be overcompensated by the advantages of faster enforcement, which would lead to less costs of type II errors.[173] However, the question remains what is the appropriate balance between fast compliance through a more rules-based rigid approach and reducing error costs through making better decisions by allowing for more flexibility. This problem also emerges in the Art. 6 DMA obligations, which also the Commission views as being susceptible to further specification (e.g., through a regulatory dialogue between the Commission and the gatekeepers). Such a process of further

169 See Caffarra/Scott Morton (2021).

170 See, e.g., Cabral et al. (2021, 11), Zimmer/Göhsl (2021, 54)

171 See, e.g., Caffarra/Scott Morton (2021), de Streel et al. (2021b, 90), Digital Regulation Project (2021c, 13).

172 See, e.g., Schweitzer (2021), Monti (2021, 11).

173 See for an analysis of the DMA proposal from the "rules vs. standards" approach Kerber (2021c); see also Schweitzer (2021), and Larouche/de Streel (2021).

specification leads, on the one hand, to the possibility of a more targeted specification for ensuring the effectiveness of the obligations; on the other hand, the same process also offers the gatekeepers the chance to delay and water-down the effectiveness of the obligations. Therefore, also this built-in limited flexibility in Art. 6 obligations, which for many of these obligations is unavoidable, has ambivalent effects on the effectiveness of the enforcement of the DMA. An additional problem is that - due to the non-applicability of the mostly economics-based assessment concepts of traditional competition law in the DMA - it is so far not clear, how the new assessment concepts and methods should look like that have to be used in the DMA for deciding on the effectiveness of compliance. This problem increases, if a more flexible approach is chosen.[174] After the following analysis and discussion of some of the obligations in the next sections we will come back to this problem as part of our overall assessment of the DMA in section 3.3.8.

3.3.4 Analysis of obligations I: Data combination and protecting choice regarding personal data: Art. 5(a) DMA and beyond

3.3.4.1 The obligation of Art. 5(a) DMA and its problems

Very important for the relationship between competition law and data protection law is certainly Art. 5(a) DMA, because it imposes the remedy of the German Facebook case, i.e. an additional consent for the combination of personal data from different sources, as a general obligation on all gatekeepers as a per-se rule without any specific assessment or balancing of effects:

> "In respect of each of its core platform services ..., a gatekeeper shall: (a) refrain from combining personal data sourced from these core platform services with personal data from any other service offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679."[175]

In recital 36, the Commission offers a competition rationale for this obligation:

> "The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry. To ensure that gatekeepers do not

174 See Kerber (2021c, 33).
175 Art. 5(a) DMA.

> unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative. The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third-party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner."[176]

Although addressing this problem of data combination in the DMA through such an obligation was broadly welcomed, a number of critical issues have been raised with respect to unclear aspects and the specific design of this obligation, which have led to various, partly far-reaching, suggestions for amendments.[177] In the following, we will analyze the complexity of the problems with the current version of Art. 5(a) in a step-by-step process.

Particularly important are the concerns, which are also relevant for the remedy in the German Facebook case, that consumers with respect to this additional consent ,ight have the same problems as in many other contexts, in which they should give consent according to the GDPR. This refers to the market failure of information and behavioral problems and the danger that they might not be capable of making a rational and informed decision or getting nudged into consent through manipulative designs of choice architectures (dark pattern behavior) through the gatekeepers. The Commission tries to consider this by requiring that this choice "should be proactively presented to the end users in an explicit, clear and straightforward manner" (recital 36), but it is unclear what this means exactly and whether it is sufficient for solving the problem. A number of commentators have raised these concerns.[178] In the Draft Opinion of the JURI Committee of the European Parliament, this problem was seen as so serious that it was proposed that such combinations of personal data through gatekeepers should be directly prohibited (without giving the option of a consent).[179] Based upon our discussion on this market failure problem in section 2.3.1 we also think that this is a very serious problem and that the concerns are justified. One option for dealing with this issue is to include additional

---

176 Recital 36, DMA.

177 See, e.g., Podszun (2021), de Streel (2021b, 59), Zimmer/Ghösl (2021, 42), Graef (2021).

178 See vzbv (2021, 10), EDPS (2021, 10), Podszun (2021, 3-7), de Streel et al. (2021b, 59), Graef (2021).

179 See JURI (2021), Amendment 40 with the justification: "As proven by the GDPR, simple consent regimes are often insufficient to address the loss of control over personal data by users. In order to limit the potential negative consequences for end users, business users and competing services, it is necessary to prevent them from combining personal data."

provisions in the DMA, e.g., against dark pattern behaviour, as it has been suggested in the discussion.[180]

A second critical question is whether this remedy of requiring an additional consent from the consumers is an effective remedy with respect to solving the competition problems, i.e. the exclusionary effects and the increasing of entry barriers through data combination (as described in recital 36), e.g., on the market for this core platform service. The main problem is that this remedy has only an effect on the competitive advantage of gatekeepers, if a large number of consumers reject this consent. If many or the majority of end users still give consent after being offered the choice, then this remedy would only have insignificant effects on contestability and competition, and might end up as another ineffective remedy.[181] Therefore, from the perspective of the objective of contestability, a direct prohibition of the data combination as a genuine competition remedy can be expected to be much more effective.[182] Condorelli/Padilla therefore suggest that "regulators could directly limit the ability of dominant, multi-platform conglomerates to combine user data across platforms (*mandatory data unbundling*)".[183] As a consequence, the Commission runs into the problem that Art. 5(a) DMA, with its requirement of an additional consent, might be hard to defend due to its possible ineffectiveness, if contestability is the only rationale for this obligation.[184] Therefore, amending Art. 5(a) DMA by replacing it through a direct prohibition of the combination of these personal data without allowing the gatekeepers to get consent from the end users might be a more effective obligation with respect to contestability and competition.[185]

---

180 See, e.g., vzbv (2021, 10). The European Data Protection Supervisor emphasizes that the consent management should be as user-friendly as possible (EDPS 2021, 10). Posdzun (2021, 11) proposes a sophisticated rating solution with trusted "Data Guides". This can be done through a specific solution in Art. 5(a) or through the anti-circumvention rules in Art. 11 DMA.

181 See Kerber/Zolna (2021, 25-27).

182 See Kerber/Zolna (2021, 25). The problem is that the decision of the end users about giving consent will not take into account the positive effects on competition. Even if the consumers would favor more competition, they are facing a collective good problem, requiring that many consumers deny this consent. Such a prohibition would certainly reduce also more benefits of economies of scope for the gatekeeper than requiring only an additional consent, where still a number of end users might agree to the data combination, but this effect is intended for reducing the data advantages of the gatekeeper and support the contestability.

183 Condorelli/Padilla (2020, 180). In their article they view the tying of privacy policies as a platform envelopment strategy that can leverage market power from one platform to the other. It is interesting that Condorelli/Padilla discuss this option as a "privacy regulation remedy" (ibid., 180).

184 Although also the solution of the German FCO suffers from this problem of a potentially ineffective remedy with regard to exclusionary effects, its argumentation was based primarily on exploitative abuse and the lack of choice, for which the remedy might be more effective, if consumers can make a well-informed choice (see Kerber/Zolna, 2021, 26).

185 Art. 5(a) DMA can therefore also be interpreted as a "data separation default solution", and the question is whether it only should be a default solution with the option that the gatekeeper can get the consent of the consumers for data combination or that it is a direct mandatory data separation solution.

3.3.4.2 Fairness for consumers: Extending the objectives to data protection and consumer protection

This raises the question about the objectives of Art. 5(a) DMA. Has this obligation also the objective of protecting consumers against the negative effects of the economic power of the gatekeeper, and therefore also intends (1) to protect against negative effects of exploitative abuse on consumers (e.g., through excessive data collection), and to strengthen (2) data (and privacy) protection, and (3) consumer policy objectives? And to what extent can Art.5(a) DMA be effective in that respect? Neither Art. 5(a) nor recital 36 give any clear hint to one of these three options. However, in section 3.3.3.1, we have seen that the objective of "fairness" in the DMA can also be interpreted as encompassing the protection against exploitative abuse, informational self-determination and privacy protection, and the freedom of choice for consumers. This would also be in line with the reasonings of the German FCO (and the German Federal Court of Justice), which focussed primarily on exploitative abusive behavior with a focus on informational self-determination, and viewed this remedy as a solution for this problem.[186] Such an interpretation is also compatible with recital 35, which emphasizes that generally the obligations "are necessary to address identified public policy concerns", mentioning explicitly the "need to safeguard public order, protect privacy and fight fraudulent and deceptive commercial practices".[187] Therefore, Art. 5(a) DMA should also encompass the protection of consumers against unfair privacy policies of gatekeepers for strengthening the protection of privacy and the freedom of choice of consumers. In that respect the asymmetric regulation of Art. 5(a) DMA could also be extended to data protection and consumer policy. However, the question is whether this clarification that Art. 5(a) DMA also intends to strengthen data protection and consumer empowerment would support the current version of allowing the gatekeepers to get consent for the data combination from the end users.

Such a clarification of the objectives would, in any case, allow better answers to the following question: Is the consent that is required according to Art. 5(a) DMA the same consent as in the GDPR or can the DMA set stricter rules than the GDPR, e.g. by requiring that this choice should be presented "in an explicit, clear, and straightforward manner", by fulfilling neutrality standards with respect to the choice architecture, or even more far-reaching measures for privacy protection? If Art. 5(a) DMA also has the task of strengthening privacy protection and empowering consumers through ensuring a minimum standard of choice, then it can be appropriate to set stricter (and also clearer!) rules for gatekeepers with respect to consent, not

186 See the decisions of Federal Cartel Office (2019) and Federal Court of Justice (2020).

187 ... if "there being no alternative and less restrictive measures that would effectively achieve the same result" (DMA, recital 35).

only for solving competition problems but also regarding data protection and consumer protection. This also could imply the direct prohibition of the data combination. The potential large additional harm for consumers and privacy through the economic power of the gatekeepers would justify the stricter rules for the gatekeepers.[188]

3.3.4.3 Policy conclusions: Difficult trade off problems and the direct prohibition of data combination

Based upon these considerations the following policy option for amending the current version of Art. 5(a) DMA cand be derived (**policy option I**):
(1) Since the merging of personal data can have negative effects on both competition and privacy, it should be clarified in Art. 5(a) DMA and recital 36 that this instrument of an additional choice regarding the combination of personal data from different sources is not only important for contestability and competition but also for strengthening data protection and consumer choice against unfair practices of the gatekeepers.
(2) For solving better the market failure problems with consent, there should be stricter rules with higher requirements how to present the choice in a non-manipulative ("neutral") way.
(3) A particular difficult problem is that the gatekeepers can always try to incentivize the giving of consent to the merging of data by degrading the quality of the service in the case of denying consent. It therefore is necessary to include a rule that controls the difference between both options. One possibility is "that gatekeepers must offer end users who do not consent to data combination an alternative service which is only different in the level of personalisation resulting from the non-cumulation of data. This alternative service must otherwise be of identical quality".[189]
These clarifications and additional requirements can then be part of an amendment of the current version of Art. 5(a) DMA.

It can however also be asked whether instead of this mandatory additional consent, it would be a better solution for contestability and data protection if the combination of such personal data from different services and sources by the gatekeepers would be directly prohibited (**policy option II**).

---

188 Decoupling these rules from the GDPR has the advantage that the Commission could, e.g., also issue clear guidelines how such a choice should be presented and, e.g., also inform the consumers about the implications and risks of the merging of their personal data for enabling them to make well-informed decisions. This might help to solve the market failure through information and behavioral problems.
189 BEUC (2021, 6).

With regard to the first policy option, it is, however, not clear whether these additional requirements will work well enough in practice, and whether they are sufficient for impeding the gatekeepers to nudge the end users to give consent to the merging of these personal data. Since the combination of these sets of personal data would allow a much deeper profiling of the consumers, the risks for the consumers are much higher, and it is not clear whether the consumers can assess these additional risks. Being in favor of informational self-determination and empowering consumers by giving them more choice does not automatically lead to the conclusion that more choice is always the superior solution, because meaningful choice has preconditions that have to be fulfilled. If these preconditions cannot be ensured in a sufficient way, then additional choice does not help the consumers, and other solutions have to be found.[190] If there are serious doubts that a considerable share of the consumers would not be capable of making meaningful decisions about this consent, then this implies that, also from a data protection and consumer policy perspective, the second policy option with the direct prohibition of the combination of data without giving the gatekeepers the option of getting an additional consent from the end users, might be the better solution for the consumers and the protection of their data and privacy. In this case an obligation that directly prohibits the data combination would have positive effects on both objectives contestability and fairness (with respect to protecting consumers against unfair privacy policies).

Let us consider a bit deeper the trade off problems here: (1) It is clear that the current solution, where gatekeepers can force the consumers to give consent to the merging of their data, would be negative both for data protection and for competition.[191] This is also the reason why there is so broad support in the discussion for addressing this problem through an obligation for gatekeepers. (2) Policy option II (direct prohibition) would be the better solution for contestability compared to policy option I, because it would lead to a (perhaps much) larger reduction of the data advantages of the gatekeepers, and therefore less distortion of competition and lower entry barriers. (3) Policy option II however does not allow consumers to give their consent that gatekeepers can merge their data. This can reduce some benefits for these consumers, because it might impede an additional personalisation, and also limits their freedom of choice. (4) If, however, many consumers cannot make meaningful decisions about this choice, then their costs in form of additional privacy risks (and consumer harm) can be much larger than

---

190 See, generally, from a consumer policy perspective about the limits of choice Digital Regulation Project (2021c, 7).

191 Economists would however claim that this current solution might be the only option (among those discussed here) that would allow a larger exploitation of the advantages of data aggregation by the gatekeepers, especially with regard to economies of scope. This would be an additional trade off, which however might not be seen as relevant with regard to the objectives of contestability and fairness in the DMA. See, e.g., also de Streel (2021b, 59).

the possible benefits.[192] This implies that a complex trade off problem has to be solved, and we think that both policy option I and policy option II are policy choices that can be defended.

Our recommendation, however, is policy option II, i.e. the direct prohibition of such combiantions of data for gatekeepers. It might be that the prohibition of the merging of personal data from different sources can impede additional benefits for the consumers through more personalisation. However, we expect that these additional benefits of further personalisation will be csmall in comparison with the additional risks for the consumers through the much more comprehensive consumer profiles through the merging of these data, and that, simultaneously, the additional anticompetitive effects of the merging of these data sets might be significant. Therefore, we conclude from this balancing of effects that it might be better to directly prohibit the merging of these personal data without giving the option to the gatekeepers to get an additional consent from the consumers. We are also sceptical how many consumers are capable to make meaningful decisions in that respect regarding these core platform services of the gatekeepers. Therefore, our recommendation is that Art. 5(a) DMA should be changed in that way that the combination of these data sets is directly prohibited. This would be a classical competition law remedy (leading to data separation), which simultaneously also has positive effects on data protection and consumer protection.[193]

3.3.4.4 An additional obligation: Mandating the option to use core platform services without having to provide personal data

Our recommendation in the last section to directly prohibit the combination of personal data through gatekeepers should not be misunderstood as challenging the objective that the choice of consumers with respect to the collection and use of personal data through the large digital firms should be protected, in general. On the contrary, we think that the main problem is that regarding the large digital firms, and here in the DMA the gatekeepers, consumers do not have enough choice with respect to informational self-determination and consumer empowerment. Therefore, in this section, we will propose an additional, much more far-reaching obligation that would give the consumers a genuine choice, whether they want to provide at all personal data to the gatekeepers or not (apart from the merging of data according to Art. 5(a) DMA).

The basic idea of the German Federal Cartel Office in the Facebook case as well as the decision of the German Federal Court of Justice was that it was the lack of choice about the use

[192] This also shows that the question whether synergies or conflicts between competition and data protection exist, can depend on the existence and remediability of one of the market failures.

[193] See for a similar reasoning and solution also Graef (2021).

of personal data that was decisive for the abusive character of the privacy policy of the dominant firm Facebook. This can be interpreted as a claim that the consumers should be ensured a minimum standard of choice with respect to their personal data in such settings of market power.[194] Both the German Facebook case and the Art. 5(a) DMA prohibit only the merging of the collected personal data without additional consent. It can, however, be asked whether the consumers should have more far-reaching choice options with regard to the collecting and further processing of their personal data?[195] This question can particularly be asked with respect to the DMA, which only imposes these obligations to this small number of gatekeepers, whose economic power vis-a-vis business and end users is assumed to be particularly large.

If we assume that core platform services as social media services of Facebook or the search engine services of Google are infrastructure-like ("must have") services, which consumer cannot de facto avoid anymore due to the lack of qualitatively comparable alternative services, then the consumers are forced to accept that the gatekeepers collect their personal data for being able to use their services.[196] This implies that they also have no genuine choice of not providing their personal data, because they have no realistic other options. The lack of other options is a result of the huge economies of scale and direct and indirect network effects, which among other reasons have led to the "tipping" of these markets (and therefore to this gatekeeper power). Therefore, the question arises, whether from a data protection and consumer policy perspective the DMA also can and should have more far-reaching obligations that limit the extent and use of the collection of personal data, and therefore protect the consumers against excessive data-collection and too high privacy risks through more extensive consumer profiling. This can also imply to ensure that the consumers have the choice, whether and to what extent they have to "pay" these (de facto monopolistic) services with personal data. One option is to impose an obligation on the gatekeepers in the DMA that they have to offer also an option to the consumers to use their core platform services without having to pay with their personal data, and, instead, can use the regular way of paying for services, namely paying with money, e.g., by a monthly subscription fee (in a similar way as a subscription fee for Netflix, Spotify, or cybersecurity services as anti-virus software). The problem is that Google, Facebook, and others do not offer such payment options for their core platform services but force the consumers to pay with their personal data.

---

194 See Federal Cartel Office (2019), Federal Court of Justice (2020), Wiedemann (2021), and for this interpretation as a minimum standard of choice Kerber/Zolna (2021, 21-23).

195 Art. 5(a) DMA does not affect the extent of the collection of personal data by the gatekeepers but only the combination of these collected data sets.

196 See also Condorelli/Padilla (2020, 181).

We therefore want to make the proposal to introduce an additional obligation for the gatekeepers in the DMA, which requires that the gatekeepers have to offer different options for paying their core platform services, which would allow consumers to opt-out from being forced to provide their personal data to the gatekeepers. Both from the perspective of informational self-determination and also from a consumer policy perspective that wants to strengthen consumer empowerment by protecting consumer choice, it seems necessary to us that consumers cannot be forced to pay such essential services, which they de facto cannot avoid, with their personal data. Since the provision of these services are admittedly costly, some remuneration is necessary and justified. Although different schemes for different options are possible, a simple basic solution would be that consumers can choose between an option A, which corresponds to the current solution of "paying" with personal data without a monetary fee, and an option B, in which the service would be paid in the regular way with a monetary price without the collection and use of personal data through the gatekeeper.[197] This would allow consumers to decide with respect to their own preferences and assessment of privacy risks whether they would prefer to pay for the service in the regular way or through the provision of their personal data.

It is not possible to analyze all the implications of such a mandated choice. However, some advantages and problems can be briefly discussed:
(1) The main advantage is that with this solution the consumers could get a genuine control over their personal data, because they are not forced to “pay” with their personal data. Important is that the provision of personal data as a “counterperformance” is not necessary for the provision of the service of the gatekeeper (as long as it is not intended to be personalised). Therefore, such a solution fulfills the objective of informational self-determination and empowers consumers to make their own genuine choice regarding “their” personal data.
(2) Depending on the number of consumers who choose monetary payment instead of payment with personal data, it also leads to a smaller or larger reduction of the data advantages of the gatekeepers with respect to their competitors and reduces entry barriers.
(3) Since the monetary price that is set by the gatekeeper is critical for how expensive or cheap the privacy-friendly option (without providing personal data) is, it might be necessary that such a price is monitored and controlled for enabling a realistic choice.[198]

---

[197] The collection of some personal data might be necessary for accounting services and preventing fraud etc.. This proposal is based upon an earlier proposal in Becker (2017), who suggested mandatory rules for offering products and services that do not require the provision of personal data ("data-avoiding products"). However this sophisticated proposal was not intended to be used only in situations of market power but as a general solution for offering "data-avoiding" products.

[198] This is not an easy task. However, in all obligations where the choice of business and end users is protected, this problem of controlling whether the different options are offered under reasonable terms will emerge, as we already have seen above in our discussion about Art. 5(a) DMA with respect to policy

4) As in the discussion of the additional consent for merging the data, also this obligation would necessitate additional rules for ensuring a neutral, non-biased choice architecture that avoids "dark pattern" effects.
(5) We are very much aware that paying with a monetary price for such a service might be a sensitive issue, because there might be concerns whether consumers can afford these fees and therefore can afford the protection of their data. However we expect that these fees (if appropriately regulated) might be small and are affordable to most consumers. Additionally, it is always possible that Member States subsidize such data protection-friendly solutions for consumers with affordability problems. It would be a subsidy that supports informational self-determination and privacy protection.[199]
(6) More complex, and also particularly interesting from an economic perspective, might be the implications for the amount of data collected by such a gatekeeper, if many consumers would choose a monetary payment, because this might lead to a decrease of the overall amount of available personal data for these platforms, which again might have effects on the efficiency of matching and perhaps a lower effectiveness of targeted advertising. Since the gatekeeper is paid for its services with money, it would however not endanger its business model.

It is clear that such a proposal has to be thought through very carefully, especially because it also can be designed in different ways. Some final remarks should help to understand our broader motivation for discussing this additional obligation proposal:
1) We want to show that the remedy of an additional consent for the merging of sets of collected personal data by gatekeepers in Art. 5(a) DMA is only one example about protecting choice for consumers regarding their personal data. It is not clear why the minimum standard of choice of consumers vis-a-vis gatekeepers should not be much more far-reaching, and allow for much more granular choices. This implies that a broad range of other obligations is possible, which increase the choice of the consumers, and, at the same time, can also have positive effects on contestability and competition.

option I (see section 3.3.4.3). If we have a de facto monopoly with regard to the core platform service, it resembles the regulation of a monopoly price.

199 Also the German Datenethikkommission (2019, 106) has discussed payment models for such services, and came to the conclusion that an alternative model of monetary payment can be an ethically acceptable solution for ensuring the voluntariness of paying with data for a service. This voluntariness is necessary according to EU data protection law (see also section 3.4.2). However, the price should not be abusive and a realistic alternative to the provision of personal data from the perspective of the consumer.

2) The proposal of such a mandated option for paying the service without personal data would also be compatible with the current Art. 5(a) DMA.[200] It can be seen as an additional and complementary obligation.
3) Our specific proposal of a choice between paying with money or personal data offers also the more fundamental perspective of an exit strategy regarding the wide-spread practice of using personal data as a "counterperformance" for a service, which is the basis of the zero-price markets that have led to so many different problems.[201]

3.3.5 Analysis of obligations II: Protection of choice for end users and business users

Whereas Art. 5(a) DMA is especially relevant for the choice of end users with respect to personal data, also a number of other obligations in the DMA intend to strengthen the choice of end users and business users. These are, in particular, Art. 5(c) (freedom of business and end users to offer and use other services), Art. 5(e) (freedom of business users not to get tied from core platform services to identification services), Art. 5(f) (freedom of business and end users not to get tied from one core platform service to another), Art. 6(1)b (freedom of end users to un-install apps, unless essential to operating system or device), Art. 6(1)c (freedom of end users to allow use of third-party apps, unless threatening the integrity), and Art. 6(1)e (no technical restriction of free choice of end users for switching or multi-homing regarding software applications and services). It is not possible here to discuss in detail the possible effectiveness of these obligations and the manifold problems that might arise in the implementation process.[202]

Important is that also these provisions for the freedom of choice of business and end users can be seen as instruments for strengthening contestability and competition, because less bundling and tying (either by technical or contractual restrictions) limit the leveraging of market power to other markets, allow for more switching and multi-homing, and open more business opportunities for independent service providers. This can strengthen competition, innovation,

---

200 This is possible both in the form of an additional consent, or – alternatively – by prohibiting directly the merging of the collected personal data.

201 Economides/Lianos (2021) go even one step further: They claim that the main market failure with respect to the collection of personal data through digital platforms is caused by the non-separation of two different markets, namely the market for the core platform service and the market for personal data. This non-separation is the result of the decision of the large digital firms to offer their core platform services only through paying with personal data (as a form of tying). If these markets would be separated, i.e. consumers would pay for the service, and the gatekeepers would pay for the personal data (without being allowed to tie these two markets), then perhaps much more transparency would exist, and the heterogeneous privacy preferences of the consumers could be fulfilled better. In their reasoning also the market power and information problem play a similar crucial role as in our analysis.

202 See for a deeper analysis of these obligations, e.g., de Streel (2021b, 59-65).

and can also contribute to the contestability of core platform services. It can however, from an economic perspective, also lead to efficiency losses and limit the incentives and range of innovations for gatekeepers. From the perspective of a traditional competition assessment, this might lead to complex tradeoff problems,[203] which also would make solutions through Art. 102 TFEU difficult.

Through the additional objective of fairness, however, also the freedom of choice as an additional powerful normative criterion can be taken into account. If the free use of commercial opportunities of business users is acknowledged as an additional normative criterion (as one dimension of interpreting fairness of platforms vis-a-vis business users) as well as the freedom of choice of consumers (as part of the objectives of consumer policy), then the advantages of protecting more choice to business users and end users can overcompensate, from a normative perspective, limited losses of efficiency and innovation, especially, because we also expect that the breaking up of the closed ecosystems of the gatekeepers through these additional choice options would open up the digital markets for other innovations and competition through independent service providers. In all these obligations this emphasis of the protection of the autonomy of business users and consumers against the economic power of the gatekeepers goes much further than what can be justified by a traditional competition-related interpretation of these obligations.[204]

This is, in our view, also important for the interpretation how effective specifications for these obligations should look like. This leads us to a brief discussion about the problems of specifying and enforcing these obligations. One of the problems is, again, that the question whether and to what extent these choice options are used, especially by consumers, depends very much on the presentation of this choice to the consumers, and whether the gatekeepers use manipulative practices but also direct incentives for disencouraging business users and end users to un-install software, use the services of independent service providers instead of those of the gatekeepers etc.. This might require additional monitoring and perhaps further specification of additional conditions for ensuring an effective compliance with these obligations. It also refers again to the problem of "dark pattern" behavior.[205] An additional question is, whether, similar to our discussion with regard to Art. 5(a), in certain cases, it might be the better solution for contestability and competition, not only to offer such a choice but also to prohibit directly that

203 See, e.g., Cabral et al. (2021, 12).
204 See also Podszun et al. (2021).
205 See below section 3.3.7.

certain software is pre-installed at all or that certain services are not allowed to be bundled, even if business or end users would consent to it.

The most difficult problem, however, might be that some obligations (in particular, Art. 6(1)b and 6(1)c) need very far-reaching technical expertise for an effective monitoring and assessment whether restrictions of the un-installation of software or allowing the use of third-party apps etc. are justified due to their essentiality or their threatening of the integrity of the hardware or the operating systems. The problem is that this requires an assessment of the possibility of other technological solutions that allow for more choice. If such an assessment is not possible as part of the enforcement process, then the gatekeepers can easily circumvent these obligations through a different design of their hard- and software.[206] It is not clear to us whether such obligations can be effectively enforced within such a per-se rule regime of obligations, even if further specification is possible, or whether for these problems an experienced regulatory authority with deep technological competencies would be necessary.[207]

3.3.6 Analysis of obligations III: Access and portability of data generated by business users and end users on platforms

A particularly interesting cluster of obligations are the Art. 6(1)a, 6(1)i, and 6(1)h DMA, because they focus on a particular set of data and are closely related to each other, and should therefore be analyzed jointly. All three obligations deal with those data that are generated through the activities of the business users and end user on the platforms of the gatekeepers, which are collected by the gatekeepers and which are under their exclusive control. One wellknown example is the market place of Amazon, on which Amazon can collect all data that are provided and generated by the business users and the consumers on this market place, especially also as part of the transactions between both market sides.

This can lead to a number of problems. If the gatekeeper has a dual role as provider of this core platform service and, at the same time, also competes with the business users (as, e.g., Amazon on its market place), then the gatekeeper can use these data from the transactions of all business users with the end users for getting a competitive advantage in comparison with these business users. In recital 43 the DMA claims that benefiting from this advantage would be unfair and should be prevented. This problem is subject to competition cases against

206 See also de Streel (2021b, 62).

207 These questions have also been discussed briefly in the Furman report, in which the need for technical experts in the "digital market unit" as new regulatory authority was emphasized.

Amazon in the EU and the US.[208] A second problem is that the business users do not have enough access to these data that they have provided and generated on this platform, because the latter have exclusive control over them. This insufficient access deprives the business users from analyzing the data they have generated on the platform, which impedes their capabilities of improving their services. e.g., through data analytics, also with respect to innovation. The third problem refers to end users, who also might be interested in these data, because getting access to these data and having the option to port these data to other platforms would reduce switching costs and allow better for multi-homing.

In a first step, Art. 6(1)a clarifies that the gatekeeper is not allowed to use these data (as far as they are not publicly available) for its own competition with the business users, because this would lead to an unfair competitive advantage.[209] In a second step, Art. 6(1)i introduces a data access right with regard to these data for the business users. Important is that the gatekeeper should provide the business user "... free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data ...". [210] Important is that this could also encompass inferred data.[211] The third and last step is Art. 6(1)h, which additionally subjects these data also to a new data portability right for business users and an extended and more effective data portability right for end users: The gatekeepers have to "provide effective portability of data generated through the activity of a business user and end users and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access".[212] This data portability right of Art. 6(1)h goes far beyond the provisions of Art. 20 GDPR, because (1) also business users (and not only end users) get such a data portability right, (2) it is not limited to personal data and encompasses also data on different levels of aggregation, and (3) the gatekeeper has also to provide tools for allowing continuous and real-time access, which helps to contribute to an effective data portability. The latter is very important, because the demand for continuous and real-time portability of data as well as technically effective portability, e.g., through high quality APIs,[213] is in the center of the current discussion about how to

208 See, e.g, EU Commission (2019) and Mantzari (2021).

209 " ... To prevent gatekeepers from unfairly benefitting from their dual role, it should be ensured that they refrain from using any aggregated or non-aggregated data, which might include anonymised and personal data ... to offer similar services to those of their business users." (recital 43 DMA).

210 Art. 6(1)i DMA; it continues "... that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services provided by the business users". The same problem is also addressed (but in a less precise form) in German competition law (sect. 19 a (2) No. 6 GWB).

211 See recital 55.

212 Art. 6(1)h DMA.

213 Recital 54.

make the data portability right of Art. 20 GDPR more effective. It is remarkable that this data portability right of end users also encompasses not only personal data but also data at higher levels of aggregation. Therefore, Art. 6(1)f DMA is another example how through an additional regulation a broader but specifically defined data portability right can be introduced that goes beyond the data portability right of Art. 20 GDPR.[214]

What is the main justification of these far-reaching obligations about the limitation of the use of these data, and the far-reaching rights on access and portability of these data? Although the recitals seem to suggest that the main rationale is their contribution to competition on the platform (with respect to Art. 6(1)a and 6(1)i) and the contestability of the platform services through Art. 6(1)h, e.g. by facilitating switching, we want to suggest that it is mainly based upon fairness considerations. In our view, it is very important that the set of data that is subject to these three obligations isqualified in a very specific way: These are data that are provided or generated by the business users and end users themselves, and therefore these are "their" data, from which they should benefit and not necessarily the platform, which only has collected the data of the business and end users. Therefore, the key question is: Who should get the benefits from these data? The decisive argument is that it is a matter of fairness that those who generate these data through their activities should also get the benefits from these data. This is entirely compatible with the (above in section 3.3.3.1 discussed) approach that business users and end users should get rewarded for their efforts, which also implies that business users get a fair share of the value of "their" data. It is this fairness rationale that can explain well, why Art. 6(1)a views the use of these data by the gatekeeper in their competition with the business users as unfair.[215] From this perspective, it can also be explained very well, why according to Art.6(1)i and 6(1)h the business and end users should have a right to fully access and port all these data in real-time and in an effective way, and especially, also why this should be free-of-charge. The reason is, and this is our interpretation, that these data are primarily seen by the DMA as "their" data and not the data of the platform, i.e. they only get access to and port their "own data". The fact that they can get access to as well as port these data has certainly also positive effects on competition and innovation (as it also is emphasized, particularly, in recital 54), but it can be suggested that the main rationale is that the business users should

[214] See our earlier discussion about the problems of making the data portability right of Art. 20 GDPR more effective in section 2.3.3.

[215] The decisive point in Art. 6(1)a is not that the use of these data by the gatekeeper leads to a competitive advantage for the gatekeeper, but what kind of specific (!) advantage is unfair, because the use of many other data advantages of the gatekeepers with respect to the business users are not seen as unfair.

reap the just rewards for their services and products and can use these data for improving them and for new innovations.[216]

The reason why we are discussing this in such detail is that we want to clarify a very important point with regard to the specification and assignment of rights on data.[217] The fact that the provider of a platform is technically in a unique position to observe everything what is happening on this platform and therefore can collect all these data that are generated by the interactions between business and end users on this platform, leads to a position of exclusive control over these data by the gatekeeper. However, the fact that they have a position of exclusive de facto control over these data does not imply that they also should be automatically acknowledged as the rightful "owners" of these data. The business and end users do not have these technological possibilities due to the design of the platform by the gatekeeper. The result is this asymmetry of who controls and can benefit from these data. This asymmetry however is a result of the gatekeeper power and the dependency of the business and end users from the platform, which does not give them other options than to accept it in a take-it-or-leave-it way. This is what is viewed here as unfair, and this unfair business practice is what is intended to be corrected by "giving back" (the benefits of) these data to those who have generated them. In that respect Art. 6(1)a, i and h can be understood as obligations about the specification and assignment of the bundles of rights on these data. This implies – translated into the language of "rights on data" – that (1) the platform does not have the right to use these data for competing with the business users, and (2) the business and end users should have immediate and full access to all "their" data, also at an aggregated level, and should have the right to port all these data. This also implies - and this is very different from an essential facility reasoning or the data-sharing obligation regarding search engine data in Art. 6(1)j DMA – that the business users and end user should also be entirely free how they are using "their" data.[218]

---

216 Please note that this rationale is very different from a typical competition law rationale for access to data or sharing of data, as, e.g., in the essential facility doctrine of Art. 102 TFEU or the data-sharing obligation with regard to search engine data in Art. 6(1)j DMA, which we will briefly discuss below. In these last two examples of data access/sharing it is not necessary that the data recipients have generated these data or contributed to them. Instead, it is necessary that these data are essential for the data claimants for entering markets and being able to compete. Vice versa, the "essential" character of these data is not a precondition for Art. 6(1) i and h. The reasonings for the obligations of Art. 6(1)i and h are however closely related to the discussion about how to deal with data access claims with respect to "cogenerated data".

217 See for the application of the "bundle of rights" approach for the specification and assignment of "rights on data" Kerber (2021b).

218 See also Kerber (2021b, 19-22). We think that such an interpretation is also compatible with the implications of the fairness concept in Digital Regulation Project (2021c, 10), where it is also emphasized that with respect to the value the "platform is a co-creation of the platform itself and its users".

It is clear that this perspective is very close to the interpretation of fairness of protecting the commercial opportunities (autonomy) of business users and the autonomy (choice) and empowerment of consumers and data subjects. In the discussion about these obligations there are demands for stronger clarifications about these data and the conditions for access and portability (e.g., whether open APIs should be mandatory) for ensuring effective access and portability.[219] Here improvements are possible, although a wide interpretation of the term "effective" access or portability might solve these problems. More difficult might be the problem of personal data and the necessary compliance with the GDPR, which is explicitly mentioned in the obligations Art.6(1)i and 6(1)h. There is certainly the danger that consumers might give too easy and uninformed consent, which can lead to negative effects on privacy. It is not clear how these problems can be solved practically, especially if the objective of an effective data access and data portability regime for these data that business and end users have generated should be achieved.[220] We think that this might require far-reaching additional regulatory solutions that might go beyond what is possible in the regular processes of further specifications of these obligations in the DMA.[221]

In the discussion about amendments of the DMA, e.g. in the European Parliament, proposals were made to eliminate the data portability right for business users in Art. 6(1)h, and instead rely entirely on Art.6(1)i for the access of business users to those data that are provided and generated by the business users and their end users on the platforms of the gatekeepers.[222] Although such a strict separation between data access of business users and data portability for end users can have advantages, we think that the introduction of an explicit data portability right for business users for this kind of data might also have advantages. The decisive question is whether the data access right of Art. 6(1)i can be a full substitute for such a data portability right. This is not clear. Usually data access rights are limited with respect to the question what the data recipient is allowed to do with the data. A data portability right would usually imply that firms who have the right to port "their" data, are free to do what ever they want to do with this data, i.e. they also can combine it with other data, share (or pool) this data with other firms, and also sell them on data markets. If the data access right of Art. 6(1)i should fulfill the same function than a data portability right in Art. 6(1)h, then it should be clarified that the business users have a right to transfer the data and are not restricted how they are using this data.

---

219 See, e,g., the discussion in de Streel (2021b, 53-64).

220 See de Streel (2021b, 64); see also the recommendations in EDPS (2021, 11) for further clarifications from a data protection perspective.

221 It might be interesting to think also about alternative data governance solutions, as, e.g., data trustee solution for these types of data, for dealing better with these problems.

222 See IMCO (2021), amendments 65 and 66.

Restricting how the business users can use the data might have negative effects on innovation, and can strengthen the gatekeepers with potentially negative effects on contestability.[223]

3.3.7 Other obligations and rules relevant to data protection and consumer policy

A number of additional obligations and rules in the DMA are particularly interesting from a data protection and consumer policy perspective, but we cannot analyze them in this report in a deeper way. Therefore, only a brief overview will be given.

3.3.7.1 Interoperability (Art. 6(1)f DMA)

Particularly important but also very complex are interoperability problems. Interoperability is important both for enabling more competition by enabling access, e.g. within ecosystems, to independent service providers leading to more competition and innovation, and also to more choice for consumers. Economic theory has clarified that mandating interoperability can have positive and negative effects on innovation and the differentiation of products and services.[224] However, designing technologically closed systems without interoperability is a common strategy for defending market power positions and increasing barriers to entry. Therefore, policy strategies that increase interoperability and support technological standardization can be very important for dealing with the economic power of the large digital firms. Art. 6(1)f DMA introduces an obligation to "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services".[225] This is the obligation that has been most criticized as not going far enough. Without being able to discuss this further, we also support this critique and the demands for extending this interoperability obligation.[226] A deeper analysis of these interoperability problem shows that also general policies that support interoperability and (e.g. industry-wide) standardization can contribute very much to foster competition, innovation, and the choice of business and end users.[227] Important is

---

223 It is certainly possible from an economic perspective to discuss whether a data portability right for business users can also have negative effects. This can also be linked to the discussion about "in-situ" access rights. See Cabral et al. (2021, 22) and Parker et al. (2021, 18-22).

224 For a general overview about the economics of interoperability and the possibilities how to deal with interoperability in traditional competition law, see Kerber/Schweitzer (2017).

225 Art. 6(1)f DMA.

226 See for critical discussions of this interoperability solution and more far-reaching proposals Digital Regulation Project (2021d), de Streel 2021b, 89), Monopolkommission (2021), Cabral et al. (2021, 22), Podszun et al. (2021), BEUC (2021, 8-9).

227 Please note that the current US proposals for solving these problems try to use more directly standardisation solutions. See Digital Regulation Project (2021e, 21-23).

that interoperability and standardized interfaces (APIs) are also preconditions for the obligations for increasing the choice of business and end users (section 3.3.5) and their data access and data portability (section 3.3.6).

3.3.7.2 Search data sharing (Art. 6(1)j DMA)

Art. 6(1)j DMA is a data-sharing obligation that only applies to online search engine services. For a long time there has been a discussion in competition policy that the dominant position of the search engine of Google is not contestable anymore, because Google has such large advantages from past search queries and the interaction of the users with the search results that other search engines cannot successfully enter the search engine market and compete. This has led to proposals that Google should share these data with its much smaller competitors on the search engine market for allowing more competition and innovation.[228] This obligation implies that a gatekeeper has to provide under FRAND terms access to "ranking, query, click and view data in relation to free and paid search generated by end users" on its online search engine. This is a far-reaching obligation, because the gatekeeper has to share these data with its direct competitors for enabling them to compete with the gatekeeper (horizontal data-sharing obligation).

If such an obligation would lead to an effective competition among search engines, this can lead to many benefits and more choice for the consumers. The main concerns from a consumer and data protection perspective refer to the question whether the anonymization of those query, click, and view data that constitute personal data might be sufficient for protecting the privacy of the users of search engines. It might be very difficult how the "gatekeeper should ensure the protection of personal data of end users by appropriate means, without substantially degrading the quality or usefulness of the data"?[229] This can be one of the difficult conflicts between competition and data protection, which might require a close collaboration between the Commission and data protection authorities (see above section 2.3.4).

---

[228] See, e.g., Prüfer/Schottmüller (2017), Cabral et al. (2021, 23). For a comprehensive analysis of potential solutions for this problem see Digital Regulation Project (2021b). This analysis, however, raises the question, whether the sharing of "ranking, query, click and view" data is sufficient for enabling competition between search engines, or whether additional measures are necessary.

[229] Recital 56, DMA.

3.3.7.3 Choice, behavioral manipulation, dark patterns and anti-circumvention provisions (Art. 11 DMA)

In chapter 2 we have seen that an important aspect of the huge economic power of the large digital firms is the simultaneous existence of market power and serious information asymmetries between platforms and users, which can allow the gatekeepers to use strategies of informational and behavioral manipulation of the consumers. This can be misleading and deceptive behavior but also the use of biased choice architectures that can induce consumers to make decisions that do not fit to their preferences but favor the interests of the gatekeepers ("dark pattern").[230] This problem is not only relevant for giving consent to the combination of data (Art. 5(a) DMA) but also for a number of obligations, in which business or end users are granted rights to choose between different options, e.g. data access and portability rights, or the right to un-install software, or not getting tied to another service. In all these cases gatekeepers can present the choice in ways that influences the decisions of the users in a systematic way. Through their access to large amounts of personal data and the possibility of experimenting with different designs (and using A/B testing) gatekeeper platforms are much more capable of using such strategies than other platforms or firms.[231] So far "dark pattern" behavior can only be partly and in a very ineffective way addressed by data protection and consumer law.[232] It is therefore necessary that these large gatekeeper platforms should be subject to additional clear rules that protect the informational self-determination and autonomy of the users against these manipulative strategies of gatekeepers, as part of the strategy of more asymmetric regulation for the large digital firms.

It is one of the main problems of the DMA that this second market failure (informational and behavioral problems, including behavioral manipulation) is not addressed in a systematic way in the DMA. The provisions in Art. 11 DMA about "Anti-circumvention" of the obligations of Art. 5 and Art. 6 do not refer in any clear way to informational or behavioral manipulative strategies, like e.g. dark pattern behavior. Therefore, it is not surprising that proposals for amendments were made that the use of dark patterns and biased choice architectures, whichfavor the interests of the gatekeepers instead of the users, should be directly and explicitly prohibited as part of the anti-circumvention rules in Art. 11 DMA.[233] We welcome these proposals and also

230 See above section 2.3.1.

231 See also de Streel (2021b, 55).

232 See Martini et al. (2021). See also below sections 3.4.2 and 3.4.3.

233 See, in particular, vzbv (2021, 13-15), BEUC (2021, 10), JURI (2021), amendments 60 – 62 (with direct reference to dark patterns).

recommend them.[234] However, such a prohibition of "dark patterns" and other manipulative behaviors need not only be seen as an anti-circumvention measure with respect to the Art. 5 and Art. 6 obligations (according to Art. 11) but could also be understood as helping directly to strengthen data protection and consumer empowerment in the DMA, and could therefore also be seen as part of a consumer policy dimension of the DMA.[235] Therefore, it also can be implemented either in a separate Article, similar to Art. 13 about transparency with regard to consumer profiling,[236] or directly as an additional obligation for all gatekeepers. This would be a very important innovative step in the DMA, because it would introduce an obligation with an explicit consumer policy rationale.[237]

3.3.8 The DMA proposal: Overall assessment and general recommendations

This report cannot provide an overall assessment of the DMA proposal with regard to its suitability to deal successfully with the huge economic power of the large digital firms. Therefore, we have focussed, on the one hand, on the analysis of the DMA from the perspective of data protection and consumer policy, but, on the other hand, we also want to offer some aspects for a more general assessment, and in what direction the DMA should be improved for better achieving its objectives.

Comparison with German and UK model

Both in the literature and in our opinion, it is an open question which of the three current European models for an additional set of stricter rules for large digital firms is more suitable for solving the problems:[238] The Digital Markets Act proposal with its per-se rules regime for gatekeepers, the already enacted sect. 19a GWB for "firms with paramount significance for

---

234 See, in particular, the specific proposal of vzbv (2021b) for amending Art. 11 DMA.

235 See also the recommendation for consumer protection in Digital Regulation Project (2021a, 19) that – in order to deal with the dark pattern problem – the largest online platforms should be subject to stronger requirements than other online platforms. They "should be given specific responsibility to ensure that their choice architecture is neutral", with the additional hint that these platforms also have the resources and capabilities to demonstrate the impact of their choice architecture, e.g. by A/B testing.

236 We will not discuss here Art. 13 DMA (and recital 61) about transparency with respect to consumer profiling, although this provision is also relevant from a consumer and data protection perspective.

237 See the new obligation 5(fa) in the Compromise Amendment E (Andreas Schwab – DMA; version of 3-10-2021) of the EP: "not distort, alter or impair end-users' and business users' autonomy. decision-making, or choice via the structure, design, function or manner of operation of their online interface or any part thereof".

238 See for such comparisons,e.g., Caffarra/Scott Morton (2021), Cappai/Colangelo (2021), Witt (2021b).

competition across markets" (with a list of behaviors that can be prohibited by the German competition authority), or the UK approach of a "pro-competition regime for digital markets" with its "digital markets unit" that can also impose firm-specific codes of conduct on firms with a "strategic market status". Some international observers think that the UK approach might have particular advantages,[239] because it is (1) an ex-ante regulatory approach (in contrast to the German sect. 19a GWB), and allows (2) with its firm-specific approach to tailor the set of behavioral rules to the specific problems of the firms with "strategic market status". This might lead to a better targeting of the problems and help to avoid to prohibit behavior that are not a problem in these cases. Such a better targeting of the problems is also possible in the German approach, because the German competition authority can choose from a rather long (menu-like) list of potentially problematic (and rather broadly defined) behaviors, which behavior they deem appropriate to prohibit in a specific case.[240] Although sect. 19a GWB entails a "reverse burden of proof", it cannot be expected that this will lead to the same effects as an ex-ante regulatory approach, especially also through the explicit possibility for these firms to offer justifications. It will have to be seen what this implies, if such cases will go to courts.[241] For defending the per-se rule approach of the DMA the Commission would argue that their approach is the only one, which might lead to a fast compliance of all gatekeepers with a broad set of obligations regarding problematic behavior without the need for deep investigations and having to deal with justifications and lengthy proceedings.

Per-se rules-based approach vs. more flexibility

The discussion about the DMA has however made clear that this objective of a fast and effective compliance of the gatekeepers with all these obligations might be very difficult to achieve. First, nearly all obligations are not clear enough for giving sufficient guidance about what the gatekeepers should do or not do. Therefore, secondly, a complex process of further specification will be necessary that can lead to lengthy negotiations between the Commission and the gatekeepers. It can be expected that gatekeepers will pursue strategies of claiming compliance by implementing a certain behavior, making it necessary for the Commission to start investigations for assessing and monitoring this compliance behavior with regard to its effectiveness. At least as important will however be that both the objective of effective compliance as well as the wide-spread demands for more flexibility in the application of the obligations has put the

239 See, e.g., Caffarra/Scott Morton (2021); see for the UK approach CMA (2020b).
240 See for the German approach above section 3.2.3.
241 See, e.g., Franck/Peitz (2021, 13), Witt (2021b).

question of a more differentiated and targeted approach on the agenda.[242] This is relevant now at the legislative level but also later in the process of further specification during the implementation of the DMA. It should be clearly understood that the more flexibility and differentiation with regard to the obligations is possible, the larger might be the potential positive effects of a better targeted approach but also the danger increases that the advantages of this ex-ante per-se rules approach of the DMA of fast compliance and avoiding lengthy proceedings are getting increasingly lost.

How should the legislator and later the Commission deal with this balancing problem? We recommend to use a cautious approach, i.e. to start with a fairly strict rules-based approach that does not allow at the beginning much flexibility, and only introduce perhaps later step-by-step (and after more experience) more flexibility, which can then lead to a refining and differentiation of the set of obligations.[243] We also recommend to design the DMA with regard to the list of core platform services and thresholds and criteria for the designation of gatekeepers in such a way that primarily gatekeeper positions of this small group of large digital firms is targeted. Focussing on the huge problems that are caused by this very small number of large digital firms also allows the application of stricter rules and a more effective enforcement.[244]

Towards a stricter and broader enforcement of the DMA

A main critique of many commentators is that the current DMA proposal is too weak and lenient with respect to its enforcement vis-a-vis gatekeepers. A number of proposals have been made for stricter and faster enforcement, e.g. with respect to deadlines for compliance, and how long it can take, before the Commission can apply effective sanctions and remedies, also with respect to structural measures.[245] Without being able to discuss here these proposals, we support the demands of many scholars and also opinions in the EP for a stricter and faster enforcement. Structural remedies, as, e.g., divestitures, should be part of the regular tool-box, which the Commission can use in case of non-compliance, and should not be seen only as an

---

242 See, e.g., the demands by de Streel et al. (2021b, 88-92), Schweitzer (2021), Cabral et al. (2021), and Digital Regulation Project (2021c, 13).

243 See Kerber (2021c, 34). One option would be to allow a defence for gatekeepers that their behavior (despite violating an obligation) does have positive effects on contestability and fairness (Digital Regulation Project, 2021c, 13). See also the recent joint position paper of Germany, France and the Netherlands about a proposal to enable the imposition of additional tailor-made gatekeeper-specific obligations after a market investigation (Friends of an Effective Digital Markets Act. 2021, 3) and Schweitzer (2021).

244 See Kerber (2021c, 34). This also would align the DMA more with the UK and the German model, who focus much more narrowly on these few large digital firms.

245 See Podszun et al. (2021, 66), de Streel (2021b, 93); see also several proposals for amendments, e.g. in IMCO (2021) and JURI (2021) for a faster and more effective enforcement.

instrument of last resort (for dealing with cases of repeated systematic non-compliance) as in the current version of the DMA.[246] A particular important problem that has been raised by many commentators is that the planned size of the staff for the task force for the enforcement of the DMA is much too small for ensuring effective compliance. This is supported by the manifold insights from the analysis of specific obligations how complex their enforcement might be (also with the need of much technical expertise). This is also linked to the concerns that the Commission might not have enough investigative powers and tools for dealing with the huge information asymmetry between the gatekeepers and the Commission, which endangers an effective control of the behaviour of the gatekeepers.[247]

Therefore, it is a very difficult question to what extent we can expect that the enacted DMA (with presumably a number of amendments) can achieve its objectives and help significantly to deal with the huge challenges through the economic power of the large digital firms. It is clear that all approaches that are currently discussed in Europe (and also in the US) have a strong experimental character with a high risk of failing.[248] This leads to the following additional recommendations:

(1) The DMA has to include the perspective to evolve over time, both for learning from its mistakes, and for being capable of dealing with the dynamics of technological and economic change on digital markets. With the update mechanisms for the lists of core platform services and obligations basic preconditions for such an evolution do exist, but the proposals for a faster and more flexible use of these mechanisms should be taken very seriously. In addition, it should be taken into account that an effective compliance with a number of these obligations might make, in the medium-term, also an institutional evolution to a proper regulatory authority necessary.

(2) The DMA should not pre-empt the introduction and application of other policies and regulatory approaches for dealing with the problems of the large digital firms, i.e. it should not monopolize the search for helpful solutions. The parallel application of traditional competition law was never questioned by the DMA proposal and might contribute a lot, because it could fill important gaps that are unavoidable in such a per-se rule regime as the DMA. Particularly important is however that also the national competition laws, e.g., the German sect. 19a GWB, are not getting excluded from applying their rules to the large digital firms. Especially, the sect. 19a GWB offers a very flexible approach that might be capable of complementing the

246 See Art. 16 DMA.

247 This problem was particularly emphasized by Cabral et al. (2021, 28).

248 See for a very insightful comparison between the DMA and the current US proposals Digital Regulation Project (2021e).

enforcement of the DMA. An additional question is how the national competition authorities, private enforcement and national courts can contribute more directly to the enforcement of the DMA.[249] Due to the uncertainty about the effectiveness of this experiment DMA (also with respect to its enforcement by the Commission), it is very important that sufficient scope for other competition authorities and additional regulatory initiatives remain for dealing with the challenges of the economic power of the large digital firms. This includes specifically also the possibilities of experimentation with additional new policy approaches.[250]

Towards a more explicit consideration of data protection and consumer policy objectives in the DMA

In our analysis in chapter 2 we emphasized that the problem of the economic power of these large digital firms is based upon the combination of market power and information power, and the simultaneous existence of unsolved competition problems and unsolved information problems and manipulative practices, and that through the key role of personal data the problems with competition, data protection, and consumer protection are deeply intertwined with each other. This led to our conclusion that some form of asymmetric regulation might also be appropriate for data protection and consumer law. Although the DMA is widely interpreted as another form of competition policy, its objectives contestability and fairness as well as its explicit insistence that it pursues different legal interests than traditional competition law opens up the perspective that the DMA can also be interpreted and further developed into the direction of strengthening data protection and consumer protection of the end users. This is directly compatible with the objective that the gatekeepers, from whom the end users are dependent due to the often existing unavoidability of their core platform services, should not be allowed to exploit this imbalance of power through unfair practices vis-a-vis the consumers. Our analysis of a number of obligations has shown that data protection and consumer policy considerations, especially the emphasis on strengthening the choice of end users, do already play an important role.

It is not possible here to discuss in more detail the wider implications of such a broader normative approach for the DMA. A more explicit acceptance that the DMA also pursues objectives of consumer policy and data protection law however would help to solve a number of problems of the current proposal:

---

[249] See also the recent proposal for complementary national enforcement in the joint position paper of Germany, France and the Netherlands (Friends of an Effective Digital Markets Act. 2021, 5).

[250] We are aware that such an approach can also lead to manifold problems and conflicts, but the advantages of a process of experimentation with policy innovations might be larger in the long-term.

(1) It would help to clarify the current contradictions and confusion about the objectives, i.e. that the DMA seems to be closely competition-oriented but also wants to be something different, and distances itself from the well-established assessment approach that is used in traditional competition law (including market definition, market power / dominance, and the effects on consumer welfare as key criterion). Opening up the interpretation of the DMA more explicitly to data protection and consumer policy objectives would eliminate these contradictions and allow in a much clearer way to develop the still missing new assessment approach that will be necessary for the application of the DMA.[251]

(2) It also would allow to address in a much more direct and effective way the large problems with regard to (the unsolved) information and behavioral problems and manipulative practices of gatekeepers in the DMA. We have seen how important they are for the economic power of the large digital firms, and therefore it is not surprising that a number of proposals have been made that the DMA should also deal with the problem of "dark pattern" behavior. We are supporting these proposals.[252] Such additional rules for strengthening the sovereignty of consumers vis-a-vis gatekeepers would then shift from the fringe into the core of what the DMA wants to achieve, and therefore acknowledge much better that both market failures have to be solved. The DMA could therefore also contribute to remedy the unsolved market failure of information and behavioral problems.

(3) A much more explicit acknowledgement that the DMA pursues not only competition-related objectives but also data protection and consumer protection objectives offers also the chance to deal better with conflicts, e.g. between competition law and data protection law, because the solving of such trade offs could then be done also – at least partly - within the DMA. This also would suggest to include also experts in data protection and consumer protection into the staff that is enforcing the DMA and therefore involved in the proceedings of the further specification of the obligations.

For dealing with the complex relationship between competition law and data protection law we distinguished in section 3.1 a basic strategy I, in which competition policy tries to take into account also data protection and privacy concerns, and a basic strategy II, which is focussing on a more integrative policy approach with respect to competition, data protection, and consumer protection. If the DMA would not only take into account competition concerns but also more aspects of data protection and consumer protection, it could evolve into a more integrated

---

[251] Since the traditional economics-based assessment concept, which focuses on effects on consumer welfare, cannot be applied in the DMA, the question arises, which new assessment concept is used in the DMA. This is not clear so far. See Kerber (2021c, 33).

[252] See vzbv (2021, 13-15), BEUC (2021, 10).

regulatory approach that can deal with the huge problems of the economic power of the large digital firms with respect to all three policies with their different objectives. The DMA could therefore also be a part of this basic strategy II with its potential for a much more effective solution of the challenges through these large digital firms. The fact that so far nearly all obligations have been derived from current or past competition cases does not have to be a huge problem, because the update mechanism for new obligations would allow to supplement the list of obligations with additional ones, which might be much clearer focussed on data protection´and consumer protection issues. It however would be necessary that it is clarified in Art. 10 DMA that new obligations can also address practices of gatekeepers, which are unfair to end users.[253]

3.4 Data protection law, consumer policy, and the strategy of a more integrative policy approach

3.4.1 Introduction

In chapter 2 we have seen that it is the combination of the two market failures market power and information and behavioral problems that makes it so difficult to deal with the huge economic power of the large digital firms. Due to their superior access to personal data they also have information power, which they can use as competitive advantages with exclusionary effects and barriers to entry, and for informational and behavioral manipulation of consumers. This is closely related to the problems that consumers have large difficulties to make rational and well-informed decisions about their personal data and are therefore to a large extent unable to manage their personal data with "notice and consent" solutions. This is one of the main reasons why pure competition-oriented solutions, either within traditional competition law (section 3.2) or as part of a primarily competition-oriented ex-ante regulation as the DMA can only contribute in a limited way to the solution of the problems through the economic power of the large digital firms (basic strategy I). From our framework in section 2.2 with both market failures and both policies competition law and data protection (and consumer law) and the insight in various interaction effects between both policy regimes follows that it might be necessary that not only competition policy but also data protection law and consumer law might have to contribute to the solution of this problem. This section 3.4 has the task of analyzing – at least in a brief way – how data protection law and consumer policy can help to solve this problem, also as part of an integrative and collaborative policy approach (basic strategy II). In that respect

253 This is not entirely clear in the current version of Art. 10 DMA. See for this demand BEUC (2021, 6).

we also will pick up again our thesis about needing more asymmetric regulation of the large digital firms, i.e. we will ask whether large digital firms should also be subject to stricter requirements with respect to data protection and consumer protection.

The analysis in section 3.4 will proceed in two steps. First, we will look at the two policies data protection law (3.4.2) and consumer policy (3.4.3) and ask to what extent and in which way they could contribute more for solving the problems. It should be kept in mind that dealing with the market failure information and behavioral problems is primarily the task of consumer law and, with respect to personal data, of data protection law. Therefore, this unsolved market failure problem and the ensuing incapability of consumers to manage their personal data with "notice and consent" solution is in itself a clear sign that there might be deficits with respect to both policies. The problem of underenforcement of data protection law was already discussed in section 2.3.2 as one auf the reasons that contribute to the economic power of large digital firms. With regard to both policies we will also focus on the question how the new phenomenon of "dark patterns" might be addressed better. Whereas in this first step, these two policies will be analyzed with respect what they can contribute better unilaterally for solving the problem, in the final section 3.4.4 the analysis will be extended to the question how a more integrative and collaborative policy approach of all these policies can help to develop additional synergies and the mitigation of conflicts between these policies. Such a more holistic approach, which also intends to deal with the problem of "policy silos", can be applied to the policies themselves but also at the level of enforcement of the legal regimes and the direct collaboration of enforcement agencies.

3.4.2 Data protection law

3.4.2.1 Introduction

Privacy and data protection laws can vary considerably. EU data protection law is a human rights-based data protection law, whereas other privacy law approaches are more comparable with consumer law approaches, as seen e.g. in the US.[254] Therefore, in the EU privacy and informational self-determination are a fundamental right which leads to a specific approach that grants data subjects a set of inalienable rights regarding their personal data and establishes rules for the processing of these personal data, e.g. by giving consent to the collection and use of their personal data. In chapter 2 we have already discussed some of the problems

[254] See for the international differences of privacy laws and their implications for the relationship between competition law and data protection or privacy laws, Douglas (2021, 29-62).

that emerge with regard to the collection and use of personal data by large digital firms. Particularly important are the issues of giving voluntary and informed consent, i.e. that data subjects suffer from informational and behavioral problems or have – due to the lack of other options – no real choice. The second big problem is caused by underenforcement and legal uncertainty in data protection law.

3.4.2.2 Solving the current problem of legal uncertainty of EU data protection law with asymmetric guidelines

Several provisions of the GDPR and national data protection law can be interpreted in different ways, e.g. either strictly or less strictly. Indeterminate legal terms which are frequently used in the GDPR and in national data protection law can generally lead to case-by-case justice, but they cause legal uncertainty in the first place because they have to be interpreted and clarified by courts and data protection authorities. The same is true for the assessment of the lawfulness of data processing on the basis of balancing fundamental rights and interests. Court proceedings increase[255] and data protection authority guidelines evolve[256] but it will take much more time to bring light into the darkness. The problem of legal uncertainty, hence, lies in the very nature of the chosen regulatory model of indeterminate legal terms and balancing requirements. The counter-model of precise legal wording leads to less case-by-case justice but more legal certainty. We are not of the opinion that a change to this counter-model is necessary, but that every effort should be made to develop comprehensive guidelines for the interpretation and application of the provisions of the GDPR that are coordinated within the EU as quickly as possible. In our opinion, these guidelines should also take into account whether the regulations are applied to small and medium-sized enterprises or to very large online platforms. The risk-based approach of the GDPR not only allows for such asymmetric regulation, but even requires it. This will be explained in the following section.

---

255 See e.g. for the years 2020 and 2021 the CJEU's decisions on the GDPR from 2021: CJEU judgment of 15 June 2021 – Facebook/Gegevensbeschermingsautoriteit, C-645/19, EU:C:2021:483; CJEU judgment of 22 June 2021 – Latvijas Republikas Saeima, EU:C:2021:504; CJEU, judgment of 9 July 2020 – VQ/Land Hessen, C-272/19, EU:C:2020:535; CJEU, judgment of 16 July 2020 – Schrems II, C-311/18, EU:C:2020:559; CJEU, judgment of 6 October 2020 – La Quadrature du Net et al., C-511/18, C-512/18, C-520/18, EU:C:2020:791; CJEU, judgment of 11 November 2020 – Orange Romania/ANSPDCP, C-61/19, EU:C:2020:901; CJEU, judgment of 10 December 2020 – C-620/19, EU:C:2020:1011.

256 See e.g. the latest guidelines published by the Art. 29 Working Party: Guidelines on transparency under Regulation 2016/679 (WP 260), adopted on 29 November 2017, last revised on 11 April 2018; Guidelines on consent under Regulation 2016/679 (WP 259), adopted on 28 November 2017, last revised on 10 April 2018; Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253), adopted on 3 October 2017. See also the latest guidelines published by the European Data Protection Board: Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0; Guidelines 04/2021 on codes of conduct as tools for transfer; Guidelines 02/2021 on virtual voice assistants, version 2.0 all adopted on 7 July 2021.

3.4.2.2.1 Risk-based approach

In principle, the GDPR follows a "one-size-fits-all" approach.[257] Nevertheless, a risk-based approach underlies some of its provisions. The extent to which a risk-based approach should be integrated into the GDPR was discussed extensively during the negotiations about the GDPR[258] and is subject to a broad discussion in legal literature. The GDPR's risk-based approach does not mean that a lower risk leads to lower obligations under the GDPR but that a higher risk causes stricter obligations to apply.[259] This is true, for example, for the obligation to document processing activities pursuant to Art. 30 GDPR where an increased risk is already presumed from a headcount of 250 employees at the responsible company pursuant to para. 5; for the obligation to notify data subjects in the event of data protection breaches pursuant to Art. 34 para. 1 GDPR; and for the obligation to conduct a data protection impact assessment pursuant to Art. 35. Art. 24 para. 1 sentence 1 GDPR (choice of technical and organizational measures to be implemented) is regarded as the central norm of the risk-based approach.[260] The implementation of technical and organizational measures must also take into account the "likelihood and severity of risks to the rights and freedoms of natural persons". It follows from Art. 24 para. 1 sentence 1 GDPR that a risk analysis is to be the starting point for the determination of the concrete obligations and thus has to be carried out prior to the processing of personal data.[261] Although the term "risk" is not defined in the GDPR, indications can be drawn from recitals 75 and 76. Recital 75 indicates that a risk means, in particular, that the processing of personal data may result in physical, material or non-material damage to the data subjects.[262] Recital 75 lists numerous individual cases in which it can be assumed that the aforementioned damage will occur:

> *"Where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political*

257 Cf. with further references: Schröder (2019, 505 f.).

258 Cf. Schröder (2019, 503f.); for a detailed comparison of the different proposals of the EU institutions see: Veil (2015, 347f.)

259 Cf. Veil (2015, 351).

260 Falker (2017, 33).

261 Falker (2017, 33); Hartung (2020, 13); Lang (2019, 31); Piltz, (2018, 19).

262 See also: DSK (2018, 2); Lang (2019, 32)

opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

We are of the opinion that the risk-based approach should be a basic principle of the GDPR, meaning that the GDPR should set a minimum standard for every data controller and that the more significant the risk, the stricter the obligations should be. This risk-based approach could be realized not only by new regulation but also by interpreting the GDPR and evolving guidelines which take into account the risk which lies in the data processing and the data controller.

3.4.2.2.2 Asymmetric guidelines for the application of Art. 6(1)a GDPR

Consent needs to be given voluntarily to be effective. According to recital 42, the data subject should not suffer any disadvantages as a result of refusing or withdrawing consent.[263] When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, Art. 7 para. 4 GDPR. According to recital 43, consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such a performance. In the following section it is discussed as a first step under which circumstances a linking between consent and the performance of a contract, or a service leads to an involuntarily given consent. This mainly depends on the interpretation of the necessity criterion and the scope of Art. 7 para. 4 GDPR. As a second step it should be evaluated under which circumstances consent is given involuntarily apart from contractual relationships between the data subject and very large online platforms. The first-step discussion offers valuable arguments for the second step.

263 Cf. in this respect also: Schulz (2018, 21).

3.4.2.2.2.1 Linkage prohibition (“Koppelungsverbot”)

In former data protection law, the linkage prohibition (“Koppelungsverbot”) – while not limited to companies with market power – presupposed that the data subject did not have another (reasonable) way of obtaining an equivalent contractual performance. Today’s linkage prohibition – according to its wording – has a much broader scope.

The necessity criterion

Data processing is only covered by Article 7 para. 4 GDPR if it is not necessary for the performance of the contract. If, on the other hand, the data processing is necessary for the performance of the contract, Art. 6 para. 1 lit. b GDPR applies. Thus, the consent of the data subject is not required and Article 7 para. 4 GDPR is not relevant.[264] The interpretation of Art. 6 para. 1 lit. a GDPR, hence, has a direct impact on the interpretation of Art. 6 para. 1 lit. b GDPR. There are different views among scholars under which circumstances data processing is necessary for the performance of the contract. Some argue in favor of a restrictive interpretation to the effect that the data processing needs to be necessary for the provision of the service contractually owed by the controller.[265] It is also argued that each data processing which refers to the “specific characteristic” of the contractually owed service[266] or certain contractual clauses is necessary.[267]

A “service in exchange for data” might be justified under Art. 6 para. 1 lit. a GDPR with such a broad interpretation of the necessity criterion if the parties stipulate the data processing as the service contractually owed by the processor.[268] This is countered by the argument that the necessity of the data processing is to be determined objectively alone.[269] The requirements of Art. 6 para. 1 lit. a GDPR as well as Art. 6 para. 1 lit. b GDPR would be left solely to the discretion of the data controller if it could decide solely through the drafting of the contract which data it was allowed to process on the basis of Art. 6 para. 1 lit. a and b GDPR.[270] In this respect, we recommend a restrictive understanding of necessity, to be assessed objectively.

---

264 Frenzel (2021, 20); Stemmer (2021, 41); on this borderline between Art. 6 para. 1 lit. b and Art. 7 para. 4 GDPR cf. also: Engeler (2018, 56).

265 Thus: Stemmer (2021, 41).

266 Buchner/Kühling (2020 ,49 ff.).

267 Cf. again: Engeler, (2018, 57 f.); Buchner/Kühling (2019, 49 ff.).

268 Thus: Gierschmann (2022, 65); Schulz (2018, 30).

269 Schulz (2018, 30); critical with regard to the criterion of transparency: Klement (2019, 63); with a more differentiated view: Buchner/Kühling (2020, 51 f.); Gollan (2018, 131); also in agreement: Buchner/Kühling (2019, 51).

270 Golland (2018,131); also in agreement: Stemmer (2021, 41.1.)

Only this corresponds to the telos and history of Art. 6 para. 1 lit. a and b GDPR which give no indication that the legislator intended to make Art. 6 para. 1 lit. a GDPR and Art. 6 para. 1 lit. b GDPR stand at any disposition of the data controller.

Broad or narrow scope of the linkage prohibition

According to the prevailing legal opinion, Art. 7 para. 4 GDPR does not contain an absolute or direct linkage prohibition.[271] Rather, it must be examined in each case whether the linking of consent and performance of a contract is actually prohibited under Art. 7 para. 4 GDPR.[272] According to recital 43, sentence 2 HS. 2 and the history of Art. 7 para. 4 GDPR, the provision might be understood as a rebuttable presumption of involuntary consent in case of linking the performance of the contract to giving consent.[273] It is not clear, yet, which criteria can be considered to assess if a linking of consent and performance of a contract leads to an involuntarily given consent. For example, it may depend on whether there is access to reasonable alternatives for the service[274] or whether the controller has a particular market power or even a monopoly position. Recital 43 sentence 1 GDPR specifically speaks of an “imbalance” which could lead to an involuntarily given consent. According to its wording, recital 43 sentence 1 particularly means an imbalance between the data subject and a public authority. At the same time, however, imbalances in private relationships are also specifically addressed by Art. 7 para. 4 GDPR,[275] for example between consumers and traders or employers and employees.[276] But recital 43 is not limited to these situations of imbalance. The particular market power of an undertaking up to its monopoly position could be considered as a criterion for the assumption of an imbalance, too.[277] The vast majority of scholars assert the special market position of the controller as an indication for the assumption of an imbalance.[278] Even though recital 43 is just a means of interpreting the GDPR and market power does not generally entail

---

271 Buchner/Kühling (2020, 46); Frenzel (2021, 18); Heckmann/Paschke (2018, 95); Schulz (2018, 26); Specht-Riemenschneider (2019, 27 f.); Taeger (2019, 90); probably tending towards a different opinion: Dammann (2016, 311).

272 Stemmer (2021, 42); against this: Dammann (2016, 311).

273 Art. 29 Data Protection Working Party (2017, 9); Specht (2019, 28); see also: Heckmann/Paschke, (2018, 97).

274 Cf. e.g.: Buchner/Kühling (2019, 52 f.).; Plath (2018, 19); Taeger (2019, 85); probably critical of this: Frenzel (2021, 18).

275 Thus: Taeger (2019, 93).

276 Buchner/Kühling (2019, 44); Schantz/Wolff (2017, 512); Specht (2019, 30 ff.).

277 Schulz, (2018, 22, 37); Plath (2018, 19 f.) On the unsuitability of this criterion: Golland (2018, 132).

278 Stemmer (2021, 43); see also: Heckmann/Paschke (2018, 98); It is generally argued that power asymmetries should be brought more into the focus of data protection law, cf. e.g. Rost (2014, 76, 77); Rehak (2018); cf. for a „structural superiority“: Engeler (2021a).

an imbalance with regard to the data subject,[279] in the special situation of big tech companies which offer services that the data subject more or less depends on, and which, at the same time, benefit from the data subject's data, one could argue in favor of an imbalance between these large digital firms and the data subject.

Invalid consent apart from contract

Recital 43 sentence 1 GDPR is not limited to "consent as counter performance" but relates to the overall prerequisite of voluntary consent. An imbalance can, hence, also exist in other situations. The two market failures which we described before lead us to the assumption that such an imbalance between very large online platforms and the data subjects exists or can exist unless the data subject has the option of using the platform without consenting to the data processing. Thus, the two market failures justify a rebuttable presumption of invalid consent if the consent is given to very large online platforms which needs to be refuted e.g. through a paid option to use the platform.[280]

3.4.2.2.3 Asymmetric guidelines for the application of Art. 6(1)f GDPR

Asymmetric guidelines which take into account the imbalance between very large online platforms and the data subject could also be established with regard to Art. 6 para. 1 lit. f GDPR. Due to the specific risks for the data subject which correspond to the two market failures, it could be argued that the interest of the data subject generally outweighs the interests of the data controller when the data are processed by a very large online platform.

3.4.2.2.4 Prohibit especially dangerous data processing

If especially dangerous data processing by very large online platforms is identified, one could even think about prohibiting this as long as the information market failure is not solved. If the risk for the data subject clearly outweighs the interests in data processing and the concept of consent doesn't work due to the two market failures, the need to protect the data subject justifies a prohibition of highly dangerous data processing, e.g. as Art. 5(a) DMA prohibits the merging of data by very large online platforms.[281]

---

279 Paal (2020, 229 f.).

280 See also our recommendation in section 3.4.4.4 to introduce an additional obligation for gatekeepers that mandates the offering of a payment option for the core platform service without having to provide personal data.

281 See our recommendation in section 3.4.4.3 to change Art. 5(a) DMA into a direct prohibition of the data combination without giving the gatekeeper the option to get consent from the end users for combining the personal data.

3.4.2.2.5 Taking into account dark patterns

In section 2.3.1 we have seen that dark patterns are biased choice architectures, e.g. through default settings, which lead people to make decisions which are potentially against their individual preferences.[282] Designers of dark patterns use their design power via a web interface to influence users to make decisions that benefit them (the designers, not the users!), e.g. to have users declare their consent to data processing. One could also speak of "dark nudging".[283] Data protection law can help to reduce dark patterns. Where an incentive is given to declare consent to data processing, e.g. by using green buttons to give consent whereas the button to deny consent is colored red (preselection patterns), one could think of an (in)voluntarily given consent.[284] California has implemented a law providing that consent to data processing obtained by means of dark patterns shall be invalid.[285] A similar law or, in any case, a respective interpretation of the GDPR, could be part of the "dark pattern solution" in Europe, too. We support such a law and such an interpretation of the GDPR. However, the different kinds of dark patterns require action by various areas of law to limit them, one of which is also consumer protection law. How especially consumer protection law could respond to dark patterns should absolutely be subject to further discussion.[286]

3.4.2.3 Solving the current problem of underenforcement

As we have already discussed in chapter 2 data protection law does not only suffer from legal uncertainty but also from underenforcement. This aspect should be discussed, here, also from a data protection law perspective. It should be argued that the problem of underenforcement is a structural problem which particularly lies in the one-stop-shop principle. We will explain the problem in the following and discuss possible solutions.

Since coming into force, data protection law has been less enforced than it would have been possible, although the data protection authorities have considerable enforcement powers according to Art. 83 ff. GDPR. In this respect, the lack of enforcement of data protection law cannot be justified by a lack of enforcement instruments. Rather, the enforcement deficit lies on the one hand in the legal uncertainty inherent in data protection law and on the other hand in the lack of enforcement efforts by individual data protection authorities. This, in turn, may be

---

282 Martini/Drews/Seeliger/Weinzierl (2021, 47, 51f.).
283 Weinzierl (2020, 1, 3).
284 Martini/Drews/Seeliger/Weinzierl (2021, 47, 53).
285 14 lit. h CPRA which amends 1798.140 lit. h Nr. 1 CCPA. See also Chopra (2020).
286 See also below section 3.4.3.

due to a lack of resources, but certainly also to other reasons, most notably the effects of the "one-stop-shop principle" and the resulting complex structure of competency.

The "one-stop-shop principle" replaced the territorial principle[287] under which several supervisory authorities could have acted in cross-border data processing. The territorial principle led to efficiency losses and caused legal uncertainties which are meant to be avoided by the "one-stop-shop principle".[288] Under this principle , the supervisory authority of the main establishment or of the single establishment of the controller or processor is now competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in principle (Art. 56 para. 1 GDPR). It must, nevertheless, cooperate with the other supervisory authorities concerned according to Art. 60 to 62 GDPR. The aim of these provisions is to reach a consensus among the supervisory authorities involved, which can e.g. be achieved through mutual assistance, exchange of information and joint action.[289] If such a consensus cannot be reached, a dispute resolution procedure, the so-called consistency procedure, can be initiated pursuant to Art. 65 para. 1 lit. a GDPR, at the end of which a binding decision of the European Data Protection Board (EDPB) is issued.[290]

Under this procedure, if the lead supervisory authority does not take the appropriate action, other supervisory authorities concerned can intervene: They can raise relevant and reasoned objections regarding the draft decision which the lead supervisory authority has previously had to submit to them (Art. 60 para. 4 GDPR). If the lead supervisory authority does not follow their objections or if it rejects them as not relevant or not reasoned, the EDPB has to adopt a binding decision under Art. 65 para. 1 lit. a GDPR. The lead supervisory authority then has to "translate" this binding decision into its final decision (Art. 64 para. 6 GDPR).

This process was recently followed with regard to the Irish data protection authority (Data Protection Commission, DPC) which is responsible, e.g., for Apple, Google, Facebook, Twitter, IBM and LinkedIn. It had issued a draft decision with regard to WhatsApp Ireland Ltd.'s compliance with Art. 12 to 14 GDPR which triggered objections by no less than eight data protection authorities concerned, e.g. regarding the scope of the inquiry and the proposed enforcement measures. As no compromise was reached, the EDPB was called upon to issue a binding

---

287 In depth: Nguyen (2015, 265).

288 Wagner/Ruhmann (2019).

289 Cf. Wagner/Ruhmann (2019); CJEU judgment of 15 June 2021 – Facebook/Gegevensbeschermingsautoriteit, C-645/19, EU:C:2021:483;

290 CJEU judgment of 24 September 2019 – Google/CNIL, C-507/17, ECLI:EU:C:2019:772 = NJW 2019, 3499 para. 68; see also the Opinion of the Advocate General in Schrems II: CJEU judgment of 16 July 2020 – Schrems II, C-311/18, ECLI:EU:C:2019:1145 = BeckRS 2019, 32163 para. 155; as well as: Gerhold (2021, 1134).

decision. In its decision, the EDPB obliged the DPC to amend its draft decision with regard to the infringements of transparency, the calculation of the imposed fine and the period for the order to comply.[291]

If on the other hand the lead supervisory authority does not act at all, the procedures available to the other supervisory authorities concerned are more complex: A supervisory authority concerned can contact the lead supervisory authority as part of the scheme of mutual assistance under Art. 61 para. 1 GDPR. If the lead supervisory authority does not react, the supervisory authority concerned can adopt provisional measures under Art. 61 para. 8 sentence 1 GDPR in accordance with Art. 55 para. 1 GDPR, e.g. evidence protection measures. It can also ask the EDPB to issue an urgent binding decision under Art. 66 para. 2 GDPR.[292] However, the CJEU in a recent decision seems to have required a prior consultation in accordance with Art. 56 paras. 3 to 5 GDPR in such cases.[293] This is meant to inform the lead supervisory authority of the intentions of the supervisory authority concerned, and to enable it to adopt measures itself.[294] In addition to this mechanism, some legal scholars have argued that the urgency procedure according to Art. 60 para. 11 GDPR should apply.[295] Another possible instrument to be taken is the complaint of inactivity under Art. 66 para. 3 GDPR. This is the only instrument developed explicitly with regard to the competent supervisory authority's inactivity.[296]

As a consequence of all of these procedures, the final substantive decision lies with the EDPB.[297] However, its decision still has to be "translated" into a decision with an external effect by the lead or another competent supervisory authority. Because the EDPB does not have any powers under Art. 58 GDPR, it has to rely on these supervisory authorities'

---

291 EDPS, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021, p. 86 ff.

292 CJEU judgment of 15 July 2021 – Facebook/ Gegevensbeschermingsautoriteit, C-645/19, ECLI:EU:2021:483, para. 71.

293 Very unclear whether the CJEU maybe only demands this in cases falling under Art. 56 para. 2 GDPR, as the clear wording of the law as well as its systematics would suggest, CJEU judgment of 15 July 2021 – Facebook/ Gegevensbeschermingsautoriteit, C-645/19, ECLI:EU:2021:483, paras. 58 ff.

294 CJEU judgment of 15 July 2021 – Facebook/ Gegevensbeschermingsautoriteit, C-645/19, ECLI:EU:2021:483, paras. 60, 71.

295 Blasek (2021); Gerhold (2021, 1134).

296 Caspar (2020a, 12); critical on this: Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015, 14 f.).

297 Leaning towards this assessment as well: Gerhold (2021, 1135); von Lewinski (2017, 1487); Thiel (2021, 470). This also corresponds with the EDPB's task as defined in Art. 70 para. 1, specifically sentence 2 lit. a, lit. e alternative 1, lit. t GDPR. Against such a binding decision, an action for annulment under Art. 263 TFEU may be brought, Weber/Dehnert, ZD 2021, 63, 67; see also recital 143.

cooperation. If such a cooperation cannot be obtained, the only possible reaction is for the European Commission to start lengthy infringement proceedings under Art. 267 TFEU.[298]

In some cases, European supervisory authorities have proceeded against GAFA(M) companies or comparable platforms. However, their number is small. They are listed in the following table:

Table 1: Fines imposed on companies in the platform economy (data mainly taken from enforcementtracker.com)

Date	Amount of the fine	Country of domicile Supervision	Addressee	Brief description
2019	51,000 €	Germany	Facebook Germany GmbH	Failure to notify the competent supervisory authority in Hamburg of the data protection officer.
21.01.2019	50,000,000 €	France	Google LLC	Unlawful data processing in regards to account creation via the Android operating system. The allegations are: the lack of transparency (Art. 5 GDPR), the lack of a legal basis (Art. 6), information deficits (Art. 13, 14) as well as the vagueness and lack of unambiguity of the declaration of consent (Art. 4 No. 11).
11.03.2020	5,000,000 €	Sweden	Google LLC	Unlawful handling with regard to the right of users to have search suggestions deleted. The Higher Administrative Court in Stockholm did not uphold an appeal by Google, but reduced the amount of the fine to approximately 5 million euros.
14.07.2020	600,000 €	Belgium	Google Belgium SA	Unlawful refusal of a data subject's request to limit the discoverability of an outdated article ("dereferencing") and the lack of transparency of the request form.
16.07.2020	28 €	Hungary	Google Ireland Ltd.	Failure to respond in a timely manner to a data subject's request for information (Art. 15).
15.12.2020	450,000 €	Ireland	Twitter International Company	Failure to inform the supervisory authority of a data protection breach within the meaning of Art. 33 DSGVO
07.12.2020	35,000,000 €	France	Facebook Europe Core S.à r.l.	Specificity: The decision is based on Art. 82 of the French Data Protection Act. The storage of cookies without the consent of the data subject and the insufficient information regarding the processing of cookies are objected to. The "one-stop-shop principle“ is considered inapplicable.
07.12.2020	60,000,000 €	France	Google LLC	

298 Caspar (2020, 28).

07.12.2020	40,000,000 €	France	Google Ireland Ltd.	Special feature: The decision in both cases is based on Art. 82 of the French Data Protection Act. The storage of cookies without consent, the insufficient information regarding the processing of cookies and the defectiveness of the function to reject the storage of advertising cookies are also objected to. The "one-stop-shop principle“ is considered inapplicable.
09.04.2021	750,000 €	Netherlands	Tik Tok	Violation of the privacy of minors. Failure to provide information that is understandable and transparent for minors.
16.07.2021	746,000,000 €	Luxembourg	Amazon Europe Core S.à.r.l.	Illegal data processing operations (more concrete information currently not available). Amazon intends to seek legal remedies.

Among the listed fines, there are six fines that censure violations of the GDPR. Among these fines, the fine of the French data protection authority against Google LLC in the amount of € 50 million and the fine of the Luxembourg supervisory authority against Amazon Europe Core S.á.r.l. in the amount of € 746 million are outstanding. The Amazon case is the first case in which a data protection authority of a member state has acted, in line with the “one-stop-shop principle”. In all other cases listed, either the “one-stop-shop principle” was deemed not to apply at the time of the issuance of the notice of the fine,[299] or a fine was issued exclusively against a specific member state subsidiary that does not constitute the European head office, resulting in a smaller fine.[300] The French regulator issued three significant fines against GAFA(M) companies in December 2020, which are based on breaches of national data protection law, thus deeming the “one-stop-shop principle” inapplicable.[301]

Although the “one-stop-shop-principle” may cause more legal certainty, it leads to inconsistent law enforcement in the different member states. We thus agree with the German Federal Data Protection Commissioner (“Bundesdatenschutzbeauftragter”, BfDI) that there is a need for a European Data Protection Authority.[302] We argue in favor of a financially adequately equipped European Data Protection Authority which is competent for the data processing by very large online platforms because data processing by those very large online platforms should be controlled more carefully than less dangerous data processing. To identify potentially unlawful

299 For example, CNIL (2019)

300 For example, for the fine imposed by the Hamburg Data Protection Commissioner on Facebook Germany GmbH, cf: HmbfDI (2019, 107).

301 Haufe Online Redaktion (2020).

302 Stupp (2021).

data processing, one could also think of further reporting requirements, e.g. within the scope of Corporate Digital Responsibility.

The problems of underenforcement and legal uncertainty are very important and urgent issues that require a fast solution. If we wait another ten years to solve them, irreversible harm will be done to the informational self-determination of EU citizens. We are of the opinion that we have a similarly dramatic situation in data protection law as we have in competition law where we react with “revolutionary” changes. The same should be done in data protection law.

3.4.3 Consumer policy

From an economic perspective consumer policy has the task of remedying market failure problems that are caused by information and behavioral problems of consumers.[303] Theoretical and empirical research in information economics and behavioral economics has shown that, e.g., through asymmetric information and behavioral biases, "adverse selection" and "moral hazard" problems as well as systematic decision errors of consumers can arise, which lead to serious market failures and can harm consumers. Firms can also use misleading and deceptive information and aggressive sales practices to the detriment of consumers. The analysis in section 2.3.1 about the problems of consumers to make rational and well-informed decisions about the collection and use of personal data is only another example of the general problems that consumers can have with respect to their consumer decisions due to their limited information and limited capabilities to process information, cognitive limitations and behavioral biases.[304] Consumer policy has developed a broad set of policy instruments for protecting consumers against a wide range of those practices and specific risks that might lead to harms for consumers (and, in particular, also to specific groups of vulnerable consumers). Consumer education, certification and labelling solutions, nudging policies (e.g. through consumer-friendly default settings), mandatory regulations for disclosing information, judicial control of standard form contracts, regulations against misleading and aggressive sales practices, as well as direct regulation of minimum standards for contracts, products, and services (e.g., with respect to safety and health risks) are well-established and widely used instruments in the toolbox of consumer policy.[305]

---

303 See for easy-to-read overviews about consumer policy, also from a behavioral economics perspective, OECD (2010) and Luth (2010)

304 See Digital Regulation Project (2021a, 4).

305 See OECD (2010).

It is not possible in this report to analyze whether and to what extent the current consumer law in the EU, which consists of a number of different laws, is capable of dealing with the manifold consumer protection problems that can emerge on online platforms or how these lasw can be improved for better solving these problems. Instead, we will summarize the most important results of a recent policy report (Digital Regulation Project: Consumer protection for online markets and large digital platforms).[306] This report asks – in a general way - from a consumer protection perspective, whether online platforms create additional problems for consumer protection, which might not be covered sufficiently by current consumer law, and whether refinements of consumer law might be necessary for better remedying these problems. The authors of the report are, however, particularly interested in the additional question whether for the "largest online gatekeeper platforms"[307] additional and stricter rules with respect to consumer protection might be necessary in comparison to other online platforms. Since these large gatekeeper platforms are presumably identical with the gatekeeper platforms of the large digital firms, the research question of this report is directly linked to our policy proposal that for the large digital firms also stricter rules for data protection and consumer protection might be necessary (asymmetric regulation).[308]

The report sees four main reasons for a differential treatment of these large digital platforms:[309] (1) These gatekeepers between business users and consumers have the ability of setting the rules on their platforms and monitor and control the activities through their access to relevant data algorithmic design skills. (2) Through their immense access to consumer data and their skills in using machine learning algorithms, they can analyze these data for behavioral patterns and can use A/B testing techniques for refining their design choices for influencing consumer behavior. (3) Weak consumer protection can particularly also increase market power, which due the already existing competition concerns regarding the largest online platform is particularly problematic. (4) Since a key rationale for consumer protection is the existence of imbalances of power between a firm and its consumers, any consumer laws that are applicable equally to all firms will protect consumers not sufficiently against the greater power of the largest online platforms. Stronger regulation for these platforms would therefore benefit the consumers much more than any additional burden for these platforms. In the following analysis, the report shows for a number of problems, why these largest online platforms should

306 See Digital Regulation Project (2021a). The authors of this report are a group of economists from Europe and the U.S.
307 See ibid., 2.
308 See above section 2.4.
309 See ibid., 10.

be subject to additional and stricter consumer protection rules than other online platforms.[310] Particularly interesting for our problem is that "the largest online platforms should be given specific responsibility to ensure that their choice architecture is neutral"[311] and that they also should be subject to additional regulatory powers.[312]

The results of this report show that the combination of the power of digital platforms and the information and behavioral problems can justify asymmetric regulation in form of stricter rules for the large digital firms also in consumer law (despite its usual character as a horizontal regulation). In that respect, the "dark pattern" problem (with its use of manipulative choice architectures, also through the use of machine learning techniques, consumer data mining and A/B testing) is also very relevant for consumer protection, and should therefore also be addressed by consumer policy. Similar to data protection law it is not possible here to analyze from a legal perspective, whether and to what extent the manifold forms of "dark patterns" can be addressed in an effective way by consumer law, or how to improve consumer law in that respect. These questions are right now both in Europe and in many other countries (particularly in the US) on the agenda for research and policy-making. It seems that at least part of these "dark patterns" might be covered also by existing consumer law, but there are also many phenomena, which cannot be addressed, in addition to complex and difficult enforcement problems (e.g. with respect to evidence).[313] It is, however, very interesting that the new methods of A/B testing can, vice versa, also be used as a new instrument for consumer protection regulation, e.g. by mandating large online platforms to prove the impact of their choice architectures.[314]

However, the consumer policy discussion about helping consumer to make better decisions about the collection and use of personal data vis-a-vis the large digital firms should also look beyond the problem of "biased vs. neutral" choice architectures: (1) It is wellknown that also consumer policy can use "nudging" policies for remedying behavioral biases of consumers, e.g., by setting "privacy-friendly" defaults, and other nudging instruments, for helping consumers to better decisions in their own interests.[315] (2) Consumer policy can also use the instruments of (voluntary and mandatory) certification and labelling solutions, standardisation of

---

310 This refers e.g. to the demarcation of digital advertising, bans on payments for ranking and inclusion in "best buy" boxes, auto-renewing subscriptions, continuous real-time data portability, impeding targeting vulnerable consumers, and "policing" harmful behavior of third-party business users.

311 Ibid., 9

312 See ibid., 30.

313 See, e.g., Martini et al. (2021), Weinzierl (2020), Digital Regulation Project (2021a).

314 See Digital Regulation Project (2021a, 30).

315 See Thaler/Sunstein (2008).

disclosure information, model contracts, but also mandatory regulation of minimum standards of choice or of limiting the extent or the types of the collection and use of personal data. Also warnings about the risks of providing too many personal data or specific types of data etc. can be a part of the tool-box that can be directly applied also with respect to decisions of consumers aboutn their personal data and privacy. One additional instrument are the much discussed Personal Information Management Systems (PIMS).

3.4.4 Towards a more integrated and collaborative policy approach

In 2014 the European Data Protection Supervisor published a "Preliminary Opinion" about "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy".[316] In this prescient and much quoted paper the EDPS already very clearly analyzed the crucial role of personal data for many platform business models with "free" services, and the ensuing privacy problems. This paper did not only show how this problem is relevant in the EU for data protection law, consumer law, and competition law, it also emphasized the interfaces between competition law, consumer protection, and data protection, and suggested as next step "to explore the scope of closer coordination between regulators".[317] This is the topic that will be analyzed deeper in this last section 3.4.4.

We see our analysis in this report also as entirely in line with this pioneering contribution of the EDPS.[318] From our framework in section 2.2 about the problem of the simultaneous existence of both market failures (market power, information and behavioral problems) and the interaction effects of competition law, data protection and consumer law on competition and data protection, it could be clarified that an integrated analysis of the causes of the problems and the effects of the different policies is necessary. In several parts of our report we have seen that with respect to the huge economic power of large digital firms the competition problem cannot be analyzed and remedied independently from the problem of information and behavioral problems regarding the collection and use of personal data. Also attempts to solve the information and behavioral problems are very difficult, and do not help much, as long as the

316 EDPS (2014).

317 EDPS (2014, 38).

318 In fact, the analytical framework used in this report has its roots to some extent in an early article of one of the authors (Kerber 2016), in which (also inspired by this preliminary opinion of the EDPS) the possible contribution of the three policies competition law, consumer law and data protection law for dealing with the privacy problem has been analyzed from an economic perspective (including the conclusion of the need for an integrative approach).

large digital firms have quasi-monopolistic market power with regard to their core platform services, because the consumers do not have other realistic choice options. Therefore, both market failures have to be addressed, and this might require that competition policy and data protection law and/or consumer law (or even additional policies) have to contribute to the solution of this common problem simultaneously. One of the important theses of this report is that the problem of the huge economic power of the large digital firms cannot be successfully dealt with through the application of only one of the policies. It also implies that the objectives of data protection law and competition law cannot be achieved any more independent from each other.[319]

In our step-by-step analysis in chapter 3, we have distinguished different strategies about policy solutions for enabling both more competition and more data protection. We have seen that there might be scope also in traditional competition law for protecting consumers better with respect to data protection and privacy against the market power of large digital firms, but this scope is still not explored and might be very limited due to many unsolved problems of assessing privacy effects in competition law. The serious problems of consumers to manage their personal data cannot be solved by traditional competition law. If the DMA is interpreted primarily as a new (ex-ante) competition policy instrument, then a similar conclusion has to be drawn, i.e. that it cannot contribute much to the solution of information and behavioral problems, and therefore remains very limited in its impact on data protection and privacy. This implies that data protection law and consumer policy have to contribute for solving these problems, and we explored at least briefly, in which direction these policies can and should be developed for offering the perspective of a larger and more effective contribution. All of these approaches remain however unilateral approaches, which are not the result of some form of coordination between these policies.

From an economic policy perspective it is clear that a combination of only unilateral approaches by different policies, for solving these common problems on digital markets, might suffer from manifold problems and remain limited, particularly with respect to conflicts, gaps, and the use of synergies. A more integrative and collaborative approach, in which some form of coordination between these policies is possible, either with respect of their reforms or with their application by enforcement authorities, offers the chance of much more effective solutions.[320] How can such a more integrative and collaborative policy approach look like? What questions have to be asked, at what levels is coordination and collaboration possible, and how

319 This is also very clearly one of the main results in the report of Douglas (2021, 3).
320 See also from an economic perspective Jin/Wagman (2020).

can this be applied in practice? In the following, we distinguish (a) the level of the policies (or laws) and (b) the level of the application of the policies by enforcement authorities or courts.

Steps towards more and better coordination I: The level of policies

At the level of the policies, it can be asked, what combination of policies (laws and regulations) can be particularly helpful for a more effective solution of the problems of market power, data protection, and consumer empowerment on digital markets with personal data as key resource and the business models of the large digital firms. How can competition policy, data protection law, and consumer law be better aligned to each other for solving these problems? In a coordinated approach, policy-makers would try to look at all policies that are relevant for solving this complex problem, and would try to understand the effects of each policy on this common problem, and what each policy might be able to contribute with its remedies for solving it. This implies that it is necessary to develop a common understanding of the problem that has to be solved, the effects of the different policies on competition, data protection, and consumer protection, and what the aggregated effects of the combination of these policies are. It is therefore necessary to understand the effects of the interplay of these policies. Such a framework, as it was presented in section 2.2, can help to understand this interplay. Based upon such an analysis, it can be better understood to what extent and how the current policies do not work well and/or are not well aligned to each other, i.e. what the policy problems and the coordination problems between these policies are. This facilitates also the identification of conflicts, gaps and missed opportunities for unlocking synergies through the combination of these policies.[321]

For such analyses it is necessary that experts in competition policy, data protection law, and consumer law are collaborating in this research, as well as also experts from different disciplines, as, in particular, lawyers, economists and other social scientists, IT specialists and data scientists etc. This requires academic research and the working out of a common understanding and perspective through the experts of these different policies. It is crucial that the experts are open to go beyond their traditional "policy silos" (with their often deeply entrenched concepts and methods), and willing to develop also new innovative ways how to approach their common problems. This requires also questioning the current traditional approaches in these policies as well as asking whether other new and innovative ways for improving these policies might lead to more effective solutions. With regard to the economic power of the large digital firms, competition experts have been forced to do this in recent years, and the new innovative regulatory approaches in Europe are a result of such a difficult process. However, for such an

[321] In chapter 2 it was also shown that it is not easy to identify correctly conflicts and synergies.

integrative and collaborative approach such policy innovations should not take place within the policy silos but should be the result of a collaborative approach from experts from all policies for enabling also a better alignment of these policies for mitigating conflicts, close gaps, and, in particular, use better potential synergies through a sophisticated new combination of these policies.[322]

Very important is that such an approach can also lead to the insight that, instead of using the current policies, it might be a better approach to introduce new additional policies and regulations, which also might allow in an easier and more targeted way to solve the problems more effectively, including how to deal with conflicts and unlocking synergies. The Digital Markets Act as a new additional regulation with the specific task of dealing with the economic power of gatekeeper platforms can be understood as such a policy innovation. Our critique in section 3.3 regarding the current discussion about the DMA is that it is in danger to focus too narrowly on competition policy, and misses the opportunity to take into account also the possibilities to introduce also stricter rules for these gatekeeper platforms with respect to data protection and consumer protection as part of a more integrated regulatory approach for these large gatekeeper platforms.[323]

Steps towards more and better coordination II: The level of enforcement

At the level of enforcement agencies already a number of initiatives exist with respect to dialogue, communication, and collaboration with respect to competition law, data protection (or privacy) law and consumer protection. A brief international overview can be found in the report of Douglas showing that "recent inter-agency cooperation includes consultations on individual matters, the issuance of joint guidance, new agency collaborative agreements and more".[324] Also within the EU, consultations between competition and data protection authorities in specific competition cases do exist as well as platforms and forums for sharing information or even agreements for cooperation between agencies.[325] However, most of them refer to cooperation

---

322 The problem of "policy silos" has been raised repeatedly in this policy discussion. See e.g. Douglas (2021, 26-27), quoting from a speech of the former head of EDPS, Giovanni Buttarelli, in 2019: "We can no longer afford to observe the bureaucratic niceties and jurisprudential silos of competition, consumer and data protection law. From now on, all of these arms of the supervision of the digital economy and society need to be working together and coherently." See with respect to enforcement also Reyna (2021).

323 Other innovative new proposals are the Digital Services Act or the Data Governance Act. For all these and other policy initiatives the question arises how the current policies and these new policies are working together, and what the aggregate effects of these broad set of (old and new) policies are, e.g. also with respect to the economic power of the large digital firms.

324 Douglas (2021, 26).

325 See the examples in Douglas (2021, 26-27).

between agencies at the national level, like e.g. in the UK.[326] At the EU level, the "European Digital Clearinghouse" (hosted by academic institutions) offers a platform since 2017 for facilitating cooperation, dialogue and exchange of insights and best practices, also between authorities in competition law, data protection, and consumer protection.[327] However, it should be seen clearly that so far nearly no well-established collaboration between the enforcement authorities of these policies exist, in particularly also not between competition and data protection authorities. Overall, collaboration, information exchange and dialogue between these agencies exist only in rare cases, and the intended process of more collaboration is still in its infancy.

Instead of asking how more collaboration can be achieved practically and also supported institutionally,[328] we would like to focus at least briefly on the question, what should be the main tasks of such a collaboration from our specific perspective and with respect to the economic power of the large digital firms:

(1) Important is again that competition and data protection authorities develop a common understanding of the problems that they are dealing with on digital markets, and especially with respect to the economic power of the large digital firms. This could also help them to think about and develop a joint strategy how they can use their current instruments from both legal regimes for achieving better the objectives of both competition law and data protection law. This can also imply to coordinate which agency should deal primarily with which group of problems, which also could include a coordinated prioritization of enforcement activities.

(2) Competition authorities and data protection authorities can also collaborate much more specifically for solving particular problems, especially with respect to conflicts. In our report repeatedly problems and conflicts emerged, where we suggested that this might be solved best through a direct collaboration between these two types of authorities. This referred primarily to various kinds of data-sharing remedies in competition law or the DMA, as well as cases, in which e.g. the large digital firms use privacy protection measures as a strategy for foreclosing competitors and increasing barriers to entry. In these cases, also the development of guidelines how to solve the trade off-problems between competition and data protection might be very helpful. They might be jointly issued guidelines but can also be guidelines of one of the agencies, which are however developed in close consultation with the other agency.

---

326 See, e.g., a recent policy paper of the CMA (2021) for launching a "Digital Regulation Cooperation Forum" for more regulatory coordination between the CMA, the ICO and Ofcom in digital markets.

327 See the website of the Digital Clearinghouse https://www.digitalclearinghouse.org/ and Vezzoso (2020, 18).

328 See e.g. Reyna (2021) who distinguishes three models of cooperation: information as-hoc co-operation, structured dialogue, and integrated dialogue.

(3) A very important third level can refer to consultation and collaboration in individual cases, both in competition law and in data protection law. This might be limited to the exchange of information but can also be extended to consultations with respect to the assessment of cases, or the specification of remedies. It could even be possible that both agencies start in a coordinated way their own investigations and make both decisions, which might lead to a more effective combination of remedies for solving better competition and data protection problems.

We are fully aware that many of these suggestions are hard to implement in reality, and would often also need institutional preconditions, which so far do not exist. However, the basic idea of this last section of this report was to develop a perspective, in which direction policy-makers and enforcement authorities should look for solutions.

References

ACCC (2019). Digital Platforms Inquiry – Final Report (July 2019).

Acemoglu, D./Makhdoumi, A./ Malekian, A./Ozdaglar, A. (2020). Too Much Data: Prices and Inefficiencies in Data Markets, available at: https://economics.harvard.edu/files/economics/files/acemoglu_spring_2020.pdf

Acquisti, A./Taylor, C./Wagman, L. (2016). The Economics of Privacy, Journal of Economic Literature, 54(2), 442–492.

Albers, M./Veit, R.D. (2021). Art. 6 DS-GVO, in: Brink, Stefan; Wolff, Heinrich Amadeus (Eds.), BeckOK Datenschutzrecht, 37th edition 2021 (quoted by paragraph).

Art. 29 Data Protection Working Party (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, WP 217.

Art. 29 Data Protection Working Party (2016). Guidelines on the right to data portability (last revised on 5 April 2017), 16/EN, WP 242.

Art. 29 Data Protection Working Party (2017). Article 29 Working Party - Guidelines on consent under Regulation 2016/679 (WP 259), adopted on 28.11.2017.

Bechmann (2014), Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, Journal of Media Business Studies 2014, 21.

Becker, M. (2017): Reconciliating Data Privacy and Trade in Data - A Right to Data-avoiding Products, ZGE/International Property Journal 9, 371-393.

BEUC (2019). Access to consumers' data in the digital economy. Position paper (13/11/2019).

BEUC (2020). Google's Fitbit takeover: EU merger control proves unable to protect consumers in the digital economy, https://www.beuc.eu/publications/google%E2%80%99s-fitbit-takeover-eu-merger-control-proves-unable-protect-consumers-digital/html

BEUC (2021). Digital Markets Act proposal. Position paper (01/04/2021).

Bierekoven, C. (2017). Auftragsverarbeitung, Joint Controllership und kleines Konzernprivileg – Hinweise zur Verarbeitung personenbezogener Daten im Konzern, IT-Rechtsberater (ITRB) 2017, 282 – 285.

Binns, R./Bietti, E. (2020). Dissolving privacy, one merger at a time: Competition, data and third party tracking, Computer Law & Security Review, 36, Article 105369; https://doi.org/10.1016/j.clsr.2019.105369

Blankertz, A. (2020). How competition impacts data privacy – And why competition authorities should care, URL: https://www.stiftung-nv.de/sites/ default/files/how_competition_ impacts_data_privacy.pdf (Last Access: 20.09.2020)

Blasek, K. (2021). Anordnung des HmbBfDI gegen Facebook – Dringlichkeitsanordnung statt Zusammenarbeit und Kohärenz?“, Zeitschrift für Datenschutz-Aktuell (ZD-Aktuell) 2021, 05210.

Botta, M./Wiedemann, K. (2019). The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey, The Antitrust Bulletin, 64(3), 428–446.

Bourreau, M. et al. (2020). Google/Fitbit will monetise health data and harm consumers, VoxEU.org, 30 September.

Buchner, B. / Kühling, J. (2020). Art. 7 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Eds.), Kommentar: Datenschutz-Grundverordnung BDSG, 3rd edition 2020; quoted by paragraph.

Buiten, M.C. (2020). Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law, Journal of Antitrust Enforcement, jnaa041, https://doi.org/10.1093/jaenfo/jnaa041

Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., and Van Alstyne, M. (2021), The EU Digital Markets Act. A report from a Panel of Economic Experts, Joint Research Centre of the European Commission. doi:10.2760/139337, JRC122910.

Caffarra, C./Ryan, J. (2021). Ending the 'Data free-for all': Antitrust v. GDPR enforcement, EURACTIV.com, https://www.euractiv.com/section/digital/opinion/ending-the-data-free-for-all-antitrust-vs-gdpr-enforcement/ [last access on 06.07.2021]

Caffarra, C./Scott Morton, F. (2021), The European Commission Digital Markets Act: A translation, Vox.eu.

Calgigo (2017), The Clock is Ticking: The Truth About GDPR Compliance, https://calligo.cloud/resources/ebook/the-truth-about-gdpr-compliance

Campbell, J./Goldfarb, A./Tucker, C. (2015). Privacy Regulation and Market Structure, Journal of Economics & Management Strategy, 24(1), 47–73.

Cappai, M./Colangelo, G. (2021). Taming digital gatekeepers: the 'more regulatory approach' to antitrust law, Computer Law & Security Review 41, 2021, 105559.

Caspar, J. (2020a). Art. 65 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Eds.), Kommentar: Datenschutz-Grundverordnung BDSG, 3rd edition 2020; quoted by paragraph.

Caspar, J. (2020b). Art. 66 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Eds.), Kommentar: Datenschutz-Grundverordnung BDSG, 3rd edition 2020; quoted by paragraph.

Choi, J.P./Jeon, D-S./Kim, B-C. (2019). Privacy and personal data collection with information externalities, Journal of Public Economics, 2019, 113-124.

Chopra, R. (2020). STATEMENT OF COMMISSIONER ROHIT CHOPRA: Regarding Dark Patterns in the Matter of Age of Learning, Inc. Commission File Number 1723186 September 2, 2020; available at: https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf (last accessed on 23.09.2021)

CMA (2020a). Online platforms and digital advertising – Market study final report, URL: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf.

CMA (2020b). A new pro-competition regime for digital markets. Advice of the Digital Markets Taskforce, December 2020.

Colangelo, G./Maggiolino, M. (2019). Antitrust über alles. Whither competition law after Facebook?, World Competition, 42(3), 355-376.

Commission Nationale de l'Informatique et des Libertés (CNIL) (2019. French regulator's fine against Google LLC (press release), 21.01.2019, available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (last accessed on 23.09.2021)

Condorelli, D./Padilla, J. (2020). Harnessing Platform Envelopment in the Digital World, Journal of Competition Law & Economics, 16(2), 143-187.

Costa-Cabral, F./Lynskey, O. (2017). Family ties: the intersection between data protection and competition in EU Law, Common Market Law Review, 54(1), 11–50.

Crémer, J./Y.-A. de Montjoye/H. Schweitzer (2019), Competition policy for the digital era, Report to the Euopean Commission.

Dammann, U. (2016). Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen, in: Zeitschrift für Datenschutz (ZD) 2016, 307 – 314.

Datenethikkommission (2019). Gutachten der Datenethikkommission.

Datenschutzkonferenz (DSK) (2018). Brief Paper No. 18, 26.04.2018, pp. 1-6, available at: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (last accessed on 23.09.2021).

de la Mano, M. /Padilla, J. (2018). Big Tech Banking, Journal of Competition Law and Economics, 14, 494–526.

de Streel, A. et al. (2021a). The European Proposal for a Digital Markets Act. A First Assessment (January 2021) CERRE Assessment paper.

de Streel, A./Feasey, R./Krämer, J./Monti, G. (2021b). Making the Digital Markets Act more resilient and effective, CERRE Recommendations Paper, May 2021.

Digital Regulation Project (2021a). Consumer Protection for Online Markets and Large Digital Platforms, Policy Discussion Paper No.1 (May 20. 2021).

Digital Regulation Project (2021b). More Competitive Search Through Regulation. Policy Discussion Paper No.2 (May 20, 2021).

Digital Regulation Project (2021c). Fairness and Contestability in the Digital Markets Act, Policy Discussion Paper No.3 (July 6, 2021)

Digital Regulation Project (2021d). Equitable Interoperability: The "super tool" of digital platform governance, Policy Discussion Paper No.4 (July 13, 2021).

Digital Regulation Project (2021e). International Coherence in Digital Platform Regulation: An Economic Perspective on the US and EU Proposals, Policy Discussion Paper No.5 (August 9, 2021).

Dnes, S. (2021). Browser Tying and Data Privacy Innovation, available at: https://ssrn.com/abstract=3867625 (last access: 30/09/2021)

Douglas, E.M. (2021). Digital Crossroads: The Intersection of Competition Law and Data Privacy, Report to the Global Privacy Assembly Digital Citizen and Consumer Working Group (July 2021).

Douglas, E.M. (2020). Monopolization Remedies and Data Privacy, Virginia Journal of Law & Technology, 24(2), 33-67.

Economides, N./Lianos, I. (2021). Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective, Journal of Competition Law and Economics. nhab007, https://doi.org/10.1093/joclec/nhab007

EDPS (2014). Preliminary Opinion of the European Data Protection Supervisor – Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, URL: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (Last Access: 20.09.2020)

EDPS (2021). Opinion 2/2021 on the Proposal for a Digital Markets Act (10 February 2021).

Efroni, Z./Metzger, J./Mischau, L./Schirmbeck, M. (2019). Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing, EDPL, 2019, 352-366.

Engeler, M. (2018). Das überschätzte Kopplungsverbot – Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen, in: Zeitschrift für Datenschutz (ZD) 2018, 55 - 62.

Engeler, M. (2021a). Tweet from 21.06.2021; available at: https://twitter.com/MalteEngeler/status/1407055064242479106 (last accessed on 23.09.2021)

Engeler, M. (2021b). Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), 20.04.2021, available at: https://www.bundestag.de/resource/lob/836166/e95c01bdb37ed9f6c08ef027cd902e47/19-9-1056_Stellungnahme_SV_Dr-_Engeler_oeATTDSG_21-04-2021-data.pdf (last acessed on 23.09.2021).

EU Commission (2020a). Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

EU Commisision (2020b). Communication "A European strategy of data", COM(2020) 66 final (19.2.2020).

EU Commission (2020c). Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions, Press release (17 December 2020).

EU Commission (2019). Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon (Press release, 17 July 2019, http://europa.eu/rapid/press-release_IP-19-4291_en.htm.

European Union (2020). OECD: Consumer data rights and competition – Note by the European Union, DAF/COMP/WD(2020)39.

Falker, F. (2017). Risikomanagement unter der Datenschutz-Grundverordnung, in: Jürgen Taeger (Ed.), Tagungsband Herbstakademie 2017, Deutsche Stiftung für Recht und Informatik (DSRI), Prof. Dr. 29 – 42.

Federal Cartel Office (2021). Sektoruntersuchung Mobile Apps. Bericht (Juli 2021).

Federal Cartel Office (2019). Decision no B6-22/16 of 6 February 2019.

Federal Court of Justice (2020). Order of 23.06.2020, Case KVR 69/19.

Forbrukerradet (2018). Deceived by Design - How tech companies use dark patterns to discourage us from exercising our rights to privacy, URL: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design (Last access: 14.07.2021)

Franck, J.-U./Peitz, M. (2021). Digital platforms and the new § 19a tool in the German Competition Act, JECLAP 2021, 1-16, https://doi.org/10.1093/jeclap/lpab055

Frenzel, E.M. (2021). Art. 7 DS-GVO, in: Paal, Boris P./Pauly, Daniel A. (Eds.), Beck'sche Kompakt-Kommentare: Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3rd edition 2021.

Furman, J./Coyle, D./Fletcher, A./Marsden, P./McAuley, D. (2019). Unlocking digital competition. Report of the Digital Competition Expert Panel.

Gal, M.S./ Aviv, O. (2020). The Competitive Effects of the GDPR, Journal of Competition Law and Economics, 16(3), 349-391.

Geradin, D. (2021). What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a Digital Markets Act?, available at http://dx.doi.org/10.2139/ssrn.3788152.

Geradin, D./Katsifis, D./Karanikioti, T. (2020). Google as a de facto regulator: Analyzing Chrome's removal of third-party cookies from an antitrust perspective, TILEC Discussion Paper DP 2020-034, 2020.

Gerhold, M. (2021). Anmerkung zum Urt. d. EuGH v. 15. Juni 2021, C-645/19", in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2021, 1125 – 1135.

Gierschmann, S. (2022). Art. 7 DS-GVO, in: Gierschmann, Sibylle; Schlender, Katharina; Stentzel, Rainer; Veil, Winfried (Eds.), Kommentar: Datenschutz-Grundverordnung, 2nd edition forthcoming in 2022; quoted by paragraph

Gill, D./Kerber, W. (2020): Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data, Competition Policy International Antitrust Chronicle, November 2020 Vol. 2(2), 54-59.

Golland, A. (2018). Das Kopplungsverbot in der Datenschutz-Grundverordnung, Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, in: Multimedia und Recht (MMR) 2018, 130-134.

Graef, I. (2020). The opportunities and limits of data portability for stimulating competition and innovation, Competition Policy International Antitrust Chronicle, November 2020 Vol. 2(2), 34-41.

Graef, I. (2021). Why End-user consent cannot keep markets contestable, https://verfassungsblog.de/blog/

Graef, I./Clifford, D./Valcke, P. (2018). Fairness and enforcement: Bridging competition, data protection, and competition law., International Data Privacy Law, 8(3), 200-223.

Graef, I. /Van Berlo, S. (2020). Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility, European Journal of Risk Regulation, https://doi.org/10.1017/err.2020.92

Greif, B. (2018), Study: Google Is the Biggest Beneficiary of the GDPR, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (HmbfDI) (2019). 28. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, 2019, available at: (last accessed on 23.09.2021)

Hartung, J. (2020). Art. 24 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Eds.), Kommentar: Datenschutz-Grundverordnung BDSG, 3rd edition 2020; quoted by paragraph.

Haufe Online Redaktion (2020). Rekordbußgelder der französischen Datenschutzbehörde gegen Google und Amazon, published on 23.12.2020, available at: https://www.haufe.de/compliance/recht-politik/google-und-amazon-erhalten-wegen-cookies-rekord-datenschutzbussen_230132_533330.html

Heckmann, D./Paschke, A. (2018). Art. 7 DS-GVO, in: Ehmann, Eugen/Selmayr, Martin (Eds.), Beck'sche Kurz-Kommentare: DS-GVO – Datenschutzgrundverordnung, 2nd edition 2018; quoted by paragraph.

Heidhues, P./Johnen, J./Koszegi, B. (2021). Browsing versus Studying: A Pro-market Case for Regulation, Review of Economic Studies 88, 708-729.

Helberger, N./Borgesius, F.Z./Reyna, A. (2017). The perfect match? A closer lookk at th relationship between EU consumer law and data protection law, Common Market Law Review 54, 1427-1466.

Ibánez Colomo, P. (2021). The Draft Digital Markets Act: a legal and institutional analysis, JECLAP 12, 561-575.

IMCO (Committee on the Internal Market and Consumer Protection) (2021). Draft report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)).

Jia, J. Jin, G.Z./Wagman, L. (2019). The Short-Run Effect of GDPR on Technology Venture Investment (May 31, 2919), http://dx.doi.org/10.2139/ssrn.3278912

Jin, G.Z./Wagman, L. (2020). Big Data at the Crossroads of Antitrust and Consumer Protection, Information Economics and Policy, Article 100865.

Johnson, G.A./Shriver, S.K. / Goldberg, S.G. (2021). Privacy & market concentration: Intended & unintended consequences of the GDPR, https://ssrn.com/abstract=3477686.

JURI (Committee on Legal Affairs) (2021). Draft opinion on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD))

Käseberg, T./Brenner, T./Füllung, D. (2021). Das GWB-Digitalisierungsgesetz im Überblick, Wirtschaft und Wettbewerb 05/2021, 269-275.

Këllezi, P. (2019). Data protection and competition law: non-compliance as abuse of dominant position, sui-generis, 2019, 343–359.

Kemp, K. (2020). Concealed data practices and competition law: Why privacy matters, European Competition Journal, 16(2–3), 628-672.

Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection, Journal of Intellectual Property Law & Practice, 11(11), 856–866.

Kerber, W. (2018). Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC (Journal of Intellectual Property, Information Technology and Electronic Commerce Law) 9(3), 2018, 310-331.

Kerber, W. (2019). Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia, available at: http://dx.doi.org/10.2139/ssrn.3469624

Kerber, W. (2021a). From (Horizontal and Sectoral) Data Access Solutions Towards Data Governance Systems, in: Drexl, J. (ed.), Data Access, Consumer Interests and Public Welfare, Nomos, 2021, 441-476. (https://dx.doi.org/10.2139/ssrn.3681263)

Kerber, W. (2021b). Specifying and Assigning "Bundles of Rights" on Data: An Economic Perspective, forthcoming in: Hofmann, F./Raue, B./Zech, H. (eds.), Eigentum in der digitalen Gesellschaft, 2021 (available at: http://dx.doi.org/10.2139/ssrn.3847620).

Kerber, W. (2021c). Taming tech giants with a per se rules approach? The Digital Markets Act from the "rules vs. standard" perspective, Concurrences No.3, 2021, 28-35.

Kerber, W. (2021d). Competition Law in Context: The Example of its Interplay with Data Protection Law from an Economic Perspective, Wirtschaft und Wettbewerb 7/8, 2021, 400-404.

Kerber, W. / Gill. D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC (Journal of Intellectual Property, Information Technology and Electronic Commerce Law) 10(2), 2019, 244-256.

Kerber, W. / Schweitzer, H. (2017). Interoperability in the Digital Economy, Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 8(1), 2017, 39 – 58.

Kerber, W. / Zolna K.K. (2021). The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law, 2021, available at: https://dx.doi.org/10.2139/ssrn.3719098.

Kesler, R. / Kummer, M. /Schulte, P. (2019), Competition and Privacy in Online Markets: Evidence from the Mobile App Industry, ZEW Discussion Paper 19-064, Mannheim.

Kettner, S./Thorun, C./Spindler, G. (2020). Innovatives Datenschutzeinwilligungsmanagement. Abschlussbericht; available at: https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1.

Klement, J.H. (2019). Art. 7 DS-GVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Eds.), Nomos Kommentar: Datenschutzrecht – DSGVO mit BDSG, 1st edition 2019; quoted by paragraph.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security, 64, 122–134.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015). Position paper: „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung“, pp. 1-16; published on 14.08.2015; available at: ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/Entschliessungen_zwischen_den_Konferenzen/20150814_Datenschutzrechtliche_Kernpunkte_fuer_die_Trilogverhandlungen_zur_Datenschutz-Grundverordnung/Kernpunktepapier_Trilog_Endfassung_DE14-08-2015.pdf (last accessed on 23.09.2021)

Körber, T. (2019). Die Facebook-Entscheidung des Bundeskartellamtes – Machtmissbrauch durch Verletzung des Datenschutzrechts?, Neue Zeitschrift für Kartellrecht, 4/2019, 187-195.

Körner, M. (2019). Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, in: Neue Zeitschrift für Arbeitsrecht (NZA) 2019, 1389 – 1395.

Krämer, J. / Senellart, P. / de Streel, A. (2020). Making Data Portability more effective for the Digital Economy (2020) CERRE report June 2020.

Lancieri, F. (2021). Narrowing Data Protection's Enforcement Gap, (August 17, 2021). Forthcoming, 74 Maine Law Review, Issue 1 (2022), http://dx.doi.org/10.2139/ssrn.3806880

Lancieri, F. / Sakowski, P.M. (2021). Competition in Digital Markets: A Review of Expert Reports, Stanford Journal for Law, Business & Finance 26, 2021, 65.

Lang, M. (2019). Art. 24 DS-GVO, in: Taeger, Jürgen/Gabel, Detlev (Eds.), Kommentar: DSGVO – BDSG, 3rd edition 2019; quoted by paragraph.

Larouche, P. / de Streel, A. (2021). The European Digital Markets Act: A Revolution Grounded on Traditions, JECLAP 12, 542-560.

Lettl, T. (2021). Der neue §19a GWB, WRP 4/2021, 413-424.

Libert, T., L. Graves, L. / Nielsen, R. (2018), Changes in Third-Party Content on European News Websites after GDPR, https://reutersinstitute.politics.ox.ac.uk/our-research/changes-third-party-content-european-news-websites-after-gdpr

Luguri, J./Strahilevitz (2021). Shining a Light on Dark Patterns, Journal of Legal Studies 13, 43-109.

Luth, H. (2010). Behavioural economic in consumer policy, Intersentis: Antwerp

Luzak (2014), Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy, Journal of Consumer Policy 2014, 547.

Lynskey, O. (2019). Grappling with "Data Power": Normative Nudges from Data Protection and Privacy, Theoretical Inquiries in Law 20, 189-220.

Mantzari, D. (2021). Power imbalances in online marketplases: At the crossroads of competition law and regulation, CLES Research Paper Series 4/2021, 6, available at: https://www.ucl.ac.uk/cles/research-papers

Marsden, P./R. Podszun (2020). Restoring Balance to Digital Competition - Sensible Rulse, Effective Enforcement, Konrad-Adenauer-Stiftung, Berlin.

Martini, M./Drews/C./Seeliger, P./Weinzierl, Q. (2021). Dark Patterns. Phänomenologie und Antworten der Rechtsordnung, Zs. für Digitalisierung und Recht, 2021, 47-74.

Moazed, A. (2019). How GDPR is Helping Big Tech and Hurting the Competition, https://www.applicoinc.com/blog/how-gdpr-is-helping-big-tech-and-hurting-the-competition/

Monopolkommission (2021). Policy Brief No.8: Ökosysteme stärker aud marktübergreifende Ökosysteme ausrichten!, 2021.

Monti, G. (2021). The Digital Markets Act - Institutional Design and Suggestions for Improvement, 2021, TILEC Discussion Paper 2021-004, vaialable at: http://dx.doi.org/10.2139/ssrn.3797730

Nguyen, A.M. (2015). Die zukünftige Datenschutzaufsicht in Europa Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO“,in: Zeitschrift für Datenschutz (ZD) 2015, pp. 265 – 270.

OECD (2020). Consumer Data Rights and Competition - Background note, URL: https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf (Last access: 14.07.2021).

Ohlhausen, M.K. (2019). Privacy and competition: Friends, foes, or frenemies? CPI Antitrust Chronicle, February 2019, 1-6.

Ohlhausen, M.K./Okuliar, A.P. (2015). Competition, Consumer Protection, and the Right (Approach) to Privacy, Antitrust Law Journal, 80(1), 121–156.

OLG Düsseldorf (2019). Order of 26.08.2019, Case VI-Kart 1/19 (V).

OLG Düsseldorf (2021). Order of 24.03.2021, Case VI-Kart 2/19 (V).

Paal, B. (2020). Marktmacht im Daten(schutz)recht, ZWeR (2), 2020, 215-244.

Parker G.G., Petropoulos G., Van Alstyne M.W. (2021). Platform Mergers and Antitrust, Working Paper 01/2021, Bruegel, forthcoming in: Industrial and Corporate Change, Special Issue on Regulating Platforms & Ecosystems (edited by Michael G. Jacobides and Ioannis Lianos).

Pfrang, S. (2019). Die Verarbeitung von Beschäftigtendaten zwischen Konzernunternehmen - Zur Reichweite eines aus der DSGVO folgenden unselbstständigen Konzernprivilegs“ in: Privacy in Germany (PinG) 2019, 159 – 163.

Plath, K.U. (2018). Art. 7 DS-GVO, in: Plath, Kai Uwe (Ed.), Kommentar: DSGVO – BDSG, 3rd edition 2018; quoted by paragraph.

Plitz, C. (2018). Art. 24 DS-GVO, in: Gola, Peter (Ed.), Kommentar: DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679, 2nd edition 2018; quoted by paragraph.

Podszun, R. (2020). Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der "Facebook"-Entscheidung des BGH, GRUR, 1268-1276.

Podszun, R. (2021). Should gatekeepers be allowed to combine data? Ideas for Art. 5(a) of the draft Digital Markets Act, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860030.

Podszun, R./Bongartz, P./Langenstein, S. (2021). The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers, EuCML, 2021, 60-67.

Prüfer/Schottmüller (2017), Competing With Big Data. TILEC Discussion Paper No. 2017-006, https://ssrn.com/abstract=2918726

Rehak, R. (2018). Was schützt eigentlich der Datenschutz? – Warum DatenschützerInnen aufhören müssen von individueller Privatheit zu sprechen (Lecture), 28.12.2018; available at: https://fahrplan.events.ccc.de/congress/2018/Fahrplan/events/9733.html

Reyna, A. (2021). Breaking Down Silos in Public Enforcement. Lessons from Consumer-Facing Markets, https://ssrn.com/abstract=3838697mimeo.

Robertson, V. (2020). Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data, Common Market Law Review, 57, 161–190.

Rost, M. (2014). 9 Thesen zum Datenschutz, in: Pohle, Jörg; Knaut, Andrea (Eds.), Fundationes I: Geschichte und Theorie des Datenschutzes, 2014, pp. 76 f.

Sabatino, L. / Sapi, G. (2019). Online privacy and market structure: An empirical analysis, DICE Discussion Paper No. 308

Schantz, P. / Wolff, H.A. (2017). Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, Schantz, Peter/Wolff, Heinrich Amadeus (Eds.), 2017; quoted by paragraph.

Schneider, G. (2018). Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook, Journal of European Competition Law & Practice, 9(4), 213–225.

Schröder, M. (2019). Der risikobasierte Ansatz in der DS-GVO – Risiko oder Chance für den Datenschutz?, Zeitschrift für Datenschutz (ZD) 2019, 503 – 506.

Schulz, S. (2018). Art. 7 DS-GVO, in: Gola, Peter (Ed.), Kommentar: DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679, 2nd edition 2018; quoted by paragraph.

Schweitzer, H. (2021). The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal, ZEuP, 503-544.

Schweitzer, H./Haucap, J./Kerber, W./Welker, R. (2018). Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Nomos, Baden-Baden, Germany. https://www.bmwi.de/Redaktion/DE/Publikationen/ Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.html.

Sokol, D.D./Zhu, F. (2021). Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates, USC Law Legal Studies Paper No. 21-27, https://ssrn.com/abstract=3852744

Sokol, D.D./Comerford, R. (2016). Antitrust and Regulating Big Data, George Mason Law Review, 23, 1129–1161.

Solove, D.J. (2013). Privacy Self-Management and the Consent Dilemma, Harvard Law Review, 126, 1880–1903.

Specht-Riemenschneider, L. (2019). § 9 – Verbraucherdatenschutz, in: Specht-Riemenschneider, Louisa / Mantz, Reto (Eds.), Handbuch Europäisches und deutsches Datenschutzrecht – Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, 2019; quoted by paragraph.

Specht-Riemenschneider, L. (2021). Data access rights – A comparative perspective, in: Drexl, J. (ed.), Data Access, Consumer Interests and Public Welfare, Nomos, 2021, 401-438.

Specht-Riemenschneider, L./Bienemann, L. (2019). § 3.3 – Informationsvermittlung durch standardisierte Bildsymbole, in: Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Eds.), Datenrecht in der Digitalisierung, 2019; quoted by paragraph.

Spoerr, W. (2021). Art. 26 DS-GVO, in: Brink, Stefan/Wolff, Heinrich Amadeus (Eds.), BeckOK Datenschutzrecht, 37th edition 2021; quoted by paragraph.

Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist´s journey towards pervasive surveillance in spite of consumers´ preference for privacy, Berkeley Business Law Journal, 16(1), 39–101.

Stemmer, B. (2021). Art. 7 DS-GVO, in: Brink, Stefan/Wolff, Heinrich Amadeus (Eds.), BeckOK Datenschutzrecht, 37th edition 2021; quoted by paragraph.

Stigler Committee on Digital Platforms (2019). Final Report, https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf

Stucke, M.E. (2018). Should we be concerned about Data-Opolies?, Georgetown Law Technology Review, 2, 275–324.

Stupp, C. (2021). Discontent Simmers Over How to Police EU Privacy Rules - Delay in WhatsApp fine highlights some EU regulators' dissatisfaction with GDPR enforcement", in: Wallstreet Journal, 13.09.2021, https://www.wsj.com/articles/discontent-simmers-over-how-to-police-eu-privacy-rules-11631525401

SVRV (Sachverständigenrat für Verbraucherfragen) (2021). Gutachten zur Lage der Verbraucherinnen und Verbraucher, April 2021.

Taeger, J. (2019). Art. 7 DS-GVO, in: Taeger, Jürgen; Gabel, Detlev (Eds.), Kommentar: DSGVO – BDSG, 3rd edition 2019; quoted by paragraph.

Thaler, R.H./Sunstein, C.R. (2008). Nudge: Improving Decisions about Health, Wealth and Happiness, Yale University Press.

Thiel, B. (2021). Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene - Eine erste Bilanz zu Kooperations- und Kohärenzverfahren, in: Zeitschrift für Datenschutz (ZD) 2021, 467 – 470.

Thomas, S. (2005). Konzernprivileg und Gemeinschaftsunternehmen – Die kartellrechtliche Beurteilung konzerninterner Wettbewerbsbeschränkungen mit Gemeinschaftsunternehmen, Zeitschrift für Wettbewerbsrecht (ZWeR) 2005, 236 – 259.

Thomas, S. (2020). § 36 GWB, in: Immenga, Ulrich/Mestmäcker, Ernst-Joachim/Körber, Torsten/Schweitzer, Heike/Zimmer, Daniel (Eds.), Kommentar: Wettbewerbsrecht – Volume 3, 6th edition 2020; quoted by paragraph

TRL (2017). Access to In-Vehicle Data and Resources – Final Report.

Turow, J./Hennessy, M./Draper, N.A. (2015). The Tradeoff Fallacy – How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation (June 26, 2015), https://ssrn.com/abstract=2820060.

United States (2020). OECD: Consumer data rights and competition – Note by the United States, DAF/COMP/WD(2020)39.

Veil, W. (2015). DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme“, Zeitschrift für Datenschutz (ZD) 2015, 347 – 352.

Vezzoso, S. (2020). All happy families are alike: The EDPS' bridges between competition and privacy, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3519974>

Vezzoso, S. (2021). The dawn of pro-competition data regulation for gatekeepers in the EU, European Competition Journal 17/2, 391-406.

Voigt, P. (2017). Konzerninterner Datentransfer – Praxisanleitung zur Schaffung eines Konzernprivilegs, Computer und Recht (CR) 2017, 428 – 433.

Volmar, M.N./Helmdach, K.O. (2018). Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office’s Facebook investigation, European Competition Journal, 14(2–3), 195–215.

von Lewinski, K. (2017). Datenaufsicht in Europa als Netzwerk, in: Neue Zeitschrift für Verwaltungsrecht (NvWZ), 2017, 1483 – 1490.

vzbv (2021). Empower consumers and lift contestability: Position paper of the Federation of German Consumer Organisations (vzbv) on the European Commission’s proposal for a rgulation on contestable and fair markets in the digital sector (Digital Markets Act) (May 04, 2021).

Wagner, B./Ruhmann, M. (2019). Irland: Das One-Stop-Shop-Verfahren, in: Zeitschrift für Datenschutz-Aktuell (ZD-Aktuell) 2019, 06546.

Waldman; A.E. (2020). Cognitive Biases, Dark Patterns, and the 'Privacy Paradox', Current Opinion in Psychology 31, 105-109.

Weber, M. P. / Dehnert, H. (2021). Das Kooperations- und Kohärenzverfahren vor dem EDSA - Praktische Erfahrungen aus dem ersten Streitbeilegungsverfahren in Sachen Twitter, in: Zeitschrift für Datenschutz (ZD) 2021, 63 – 68.

Weinzierl, Q. (2020). Dark Patterns als Herausforderung für das Recht., Neue Zeitschrift für das Verwaltungsrecht Extra 15/2020, 1-11.

Wettbewerbskommission 4.0 (2019). Ein neuer Wettbedwerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0 (September 2019).

Wiedemann, K. (2021). Zum Zusammenspiel von Datenschutzrecht und Kartellrecht in der Digitalökonomie, CR 2021, 425-432.

Witt, A.C. (2021a). Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case, The Antitrust Bulletin, 66(2), 276-307.

Witt, A.C. (2021b). Platform regulation in Europe – per se rules to the rescue?, mimeo.

Wurzberger, S. (2017). Anforderungen an Betriebsvereinbarungen nach der DS-GVO - Konsequenzen und Anpassungsbedarf für bestehende Regelungen“, in: Zeitschrift für Datenschutz (ZD) 2017, 258 – 263.

Zimmer, D./Göhsl, J.-F. (2021), Vom New Competition Tool zum Digital Markets Act: Die geplante EU-Regulierung für digitale Gatekeeper, ZWeR 2021, 29-61.