Joint Discussion Paper Series in Economics

by the Universities of

Aachen · Gießen · Göttingen
Kassel · Marburg · Siegen

ISSN 1867-3678

No. 14-2021

Wolfgang Kerber and Karsten K. Zolna

The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law

This paper can be downloaded from
http://www.uni-marburg.de/fb02/makro/forschung/magkspapers

Coordination: Bernd Hayo • Philipps-University Marburg
School of Business and Economics • Universitätsstraße 24, D-35032 Marburg
Tel: +49-6421-2823091, Fax: +49-6421-2823088, e-mail: hayo@wiwi.uni-marburg.de

The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law

Wolfgang Kerber and Karsten K. Zolna*

(version: 26 February 2021)

Abstract: Can competition law also take into account effects on privacy or should privacy concerns of data-collecting behaviour only be dealt with by data protection law? In this paper we are analysing the German Facebook case, in which certain terms of service (that force consumers to give consent for merging personal data collected through Facebook services with those collected from tracking and third-party websites) were prohibited as exploitative abuse of a dominant firm. We show from an economic perspective that due to the simultaneous existence of two market failures (market dominance, information and behavioral problems) and complex interaction effects between both market failures and both policies in digital markets, the traditional approach of a strict separation of both policies is not possible any more, leading to the need for more collaboration and alignment of both policies. With respect to the substantive question of protecting a minimum level of choice options for consumers regarding personal data vis-a-vis dominant digital platform firms, the recent decision of the German Federal Court of Justice in the Facebook case and the proposed Digital Market Act have opened new perspectives for dealing with privacy concerns in competition law and regulation.

Key words: competition law, Facebook, digital platforms, privacy, data protection law

JEL codes: K21, K24, L40, L50

---

* Wolfgang Kerber, Professor of Economics (kerber@wiwi.uni-marburg.de); Karsten Konrad Zolna, Teaching and Research Assistant (karsten.zolna@wiwi.uni-marburg.de); Marburg Centre for Institutional Economics (MACIE), School of Business & Economics, University of Marburg (Germany). Basic ideas for this article have been developed during a research stay of Wolfgang Kerber in March 2020 as Fellow at the Weizenbaum Institute in Berlin and presented in a Weizenbaum Lecture on 3 March 2020. The authors thank Aline Blankertz, Oliver Budzinski, Filippo Lancieri, Rupprecht Podszun, Viktoria Robertson, Simonetta Vezzoso, and the participants of the 37th Annual Conference of the European Association of Law and Economics (EALE), 24-25 September 2020, and of the 16th Annual Conference of the Società Italiana di Diritto ed Economia/Italian Society of Law and Economics (SIDE-ISLE), 16-18 December 2020. The authors declare no conflict of interests.

1. Introduction

The “Facebook” decision of the German Federal Cartel Office in February 2019 is the first decision of a competition authority, in which the protection of privacy has been explicitly taken into account in a competition law decision.[1] In more detail, the Federal Cartel Office (FCO) argued that forcing users via its terms of services to give consent to the merging of personal data collected inside the social media platform Facebook and outside of it to be an exploitative abusive behavior of a dominant firm. This decision has triggered a very intense and controversial international discussion about the problem whether competition policy should also take into account effects on privacy of consumers. This case is being discussed so broadly and intensely, because it touches the so far unclarified relationship between competition law and data protection (or privacy) law under the new conditions of digital markets. This is also very important for the current discussion in competition policy about the market (and gatekeeper) power of large digital platform firms (and the need for their regulation), because their superior access to personal data is one of the most important reasons for the persistence of their market power.[2] The interim decision of the German Federal Court of Justice (Bundesgerichtshof) in this Facebook case, which supported the decision of the FCO but also developed a new reasoning based upon the constitutionally protected right on informational self-determination, as well as a proposed obligation for gatekeeper platforms in the recent proposal of the Digital Market Act (DMA) to give the users an explicit choice about the merging of personal data, have put the Facebook case even more on the agenda of the international discussion.[3]

The objective of this article is to analyze the question whether and to what extent negative effects of data-collection behaviour and privacy terms of large digital platform firms on competition and privacy can be taken into account in competition law, or whether - as the critics of the Facebook decision of the FCO claim - privacy concerns should be exclusively dealt with by data protection law (or consumer law). This widely supported position, which has also been applied in the practice of EU competition law (and many other competition law regimes), is based upon a concept of a strict separation between competition law, which should focus on solving competition problems, and data protection law, which has the task of protecting privacy, particularly with respect to market failures through information and behavioral problems of consumers. In this article we will argue that in situations like the Facebook case, in which we have simultaneously both market failure problems (market dominance plus information and behavioral problems of consumers), such a simple separation into two policies, which solve independently from each other these two market failure problems, does not work any more due to manifold interaction effects between the two market failures and between the two policies on competition and privacy. This strong intertwinement of the effects of both market failures and policies on digital markets makes the relationship between both policies difficult and complex from an economic perspective. Based upon this theoretical framework we analyse in a step-by-step approach both competition law and data protection law, leading to the conclusion that only competition law can deal

---

[1] See Bundeskartellamt (2019a).

[2] See, e.g., Crémer et al. (2019), Furman et al. (2019), ACCC (2019), Stigler Committee on Digital Platforms (2019).

[3] See Bundesgerichtshof (2020), Draft Digital Market Act, Art. 5(a) (European Commission 2020a).

with the negative effects of competition problems (e.g., cartels, mergers, dominant firms) on privacy, because data protection law is not capable of analysing and solving competition problems. Since however also competition law with its remedies can only insufficiently solve the negative effects on privacy that are caused by the combination of both market failures, a stronger collaboration and alignment of competition and data protection law is necessary for solving these problems in the context of digital markets.

Our article is structured as follows. Chapter 2 offers an overview about the broad and controversial discussion about the Facebook case and its implications for the relationship between competition and data protection law. Chapter 3 presents from an economic perspective a theoretical framework about the two market failures, two policies, and their interaction effects, applied to the effects of data-collection behaviour and privacy terms on competition and privacy. Chapter 4 shows why competition law can take into account privacy effects, and why, vice versa, data protection law is not capable of protecting consumers against negative effects on privacy through competition problems. Chapter 5 discusses in close connection with the Facebook case how privacy concerns can be considered in the control of abusive behaviour of dominant firms, and analyzes in this respect the different approaches of the FCO, the German Federal Court of Justice, and Art. 5(a) in the Digital Market Act proposal of the EU Commission. After an analysis of the problems of the remedies in the Facebook case, the concluding chapter 6 focuses on the need for a more collaborative and integrated policy approach for dealing better with the complex problems in digital markets with respect to competition, privacy, innovation, and consumer empowerment.

2. The controversial discussion about the German Facebook case

The relevance of the Facebook case of the German Federal Cartel Office (FCO) is based on the insight in the competition policy discussion that large digital platform firms as Google and Facebook have entrenched market power positions due to their superior possibilities to collect huge amounts of personal data, which gives them large competitive advantages compared to their competitors, especially on online advertising markets. Important is that they collect data not only through their own services but also through combining them with personal data from many other sources, especially also third-party websites and online tracking.[4] In its decision the FCO has challenged primarily a specific part of the terms of services of Facebook: In order for being able to use the social media platform service of Facebook, consumers also have to give consent to the collection and use of personal data from other sources. Due to this consent, Facebook can combine and use all personal data collected via its core platform service, via its other platforms (e.g. Instagram, WhatsApp) as well as via third-party websites and its other online tracking activities. In the following, we will call this requirement a "bundling of consent".[5] This allows Facebook to derive comprehensive consumer profiles for offering targeted advertising (and other services) but might also lead to large privacy risks. The decision of the FCO challenged this requirement as abusive,

---

[4] See ACCC (2019, 84-87), Binns/Bietti (2020), CMA (2020a, paras. 2.18-2.22), Robertson (2020, 162-165).

[5] The decisive point is that users cannot give consent (according to data protection law) only for data collected by using Facebook services but have to accept a bundle of consent that also encompass their personal data from manifold other sources. Condorelli/Padilla (2020) have called this bundling strategy "tying of privacy policies".

and stipulated that consumers should have an additional explicit choice whether they consent to this combination of the collected personal data or not. This implies that the consumers should also be able to use the social media platform of Facebook without such a merging of these two sets of personal data that Facebook collects through its own services and through other external sources.[6]

From a legal perspective the Facebook case can be summarized as follows.[7] The FCO did not apply Art. 102 TFEU but the German rules for the abuse of dominance (§ 19 GWB). After arguing why Facebook is dominant on the market for social media in Germany, it claimed that the above-mentioned terms of service of Facebook have to be assessed as an abusive behavior of a dominant firm. These terms lead first of all to an exploitative abuse (due to its unfair business terms infringing data protection law) and also to an exclusionary abuse. Particularly important is that the FCO uses the criterion of a violation of EU data protection law as benchmark for determining the abusive character of these terms of services.[8] After a deep assessment of these terms the FCO concluded that this requirement to consent to the combination of these two sets of personal data violates the GDPR. In that respect the FCO was also in close contact with data protection authorities, who also have supported the decision of the FCO. Due to the market dominance of Facebook (including lock-in effects of users), the users would have to accept these "take-it-or-leave-it" terms, and therefore Facebook's market power facilitates these data protection infringements. In its decision the FCO also emphasizes that due to lack of transparency the consumers are not able to understand how their data is collected and used (in particular from outside of Facebook). In combination with having not enough choice, the consumers face a “loss of control” with regard to their data. Since the dominant firm Facebook also gets through these illegal terms of services large competitive advantages through more data on other markets, especially advertising markets, this behaviour has also to be seen as an exclusionary abuse with respect to horizontal competition.[9]

This case has pioneer character in several ways. It is the first case, in which the data-collecting behaviour of digital platforms has been directly challenged as an exploitative abuse of a dominant firm in competition law, i.e. the FCO wants to protect consumers directly with regard to privacy. The practice of EU competition law has so far been very reluctant to take into account negative effects on privacy.[10] Also the direct assessment of data protection law by a competition authority and its use as a benchmark for a competition law violation is a bold and innovative step in competition law. Another innovative reasoning of the FCO is that due to the dominance of Facebook the consent of the users to the merging of their data cannot be seen as "voluntary" any more,

---

6 See Bundeskartellamt (2019b, 1-2)

7 See Bundeskartellamt (2019a).

8 The FCO chose this approach, because in Germany competition law precedent cases exist, in which the abusive character of terms and conditions has been derived from violating other laws.

9 See Bundeskartellamt (2019b, 5-6)

10 See OECD (2020, paras. 80-99), Robertson (2020, 166), Volmar/Helmdach (2018, 207) and European Union (2020, paras. 29-42).

reflecting wide-spread concerns about the loss of control of consumers over their data.[11] It also leads the FCO to the innovative remedy of requiring an additional consent for combining these data sets ("internal unbundling"). The controversial character of this case has also become apparent in the preliminary court proceedings about the Facebook decision. In August 2019 the Higher Regional Court of Düsseldorf (OLG Düsseldorf) suspended the execution of the Facebook decision in interim legal proceedings with an unusually harsh and clear rejection of many reasonings of the FCO.[12] This court decision however was equally clearly rejected by the German Federal Court of Justice (BGH) in June 2020, which fully supported the decision of the FCO but developed an own separate reasoning that deviated from the FCO, and, in particular, did not rely on a violation of EU data protection law.[13] However, the main legal proceedings in this case are ongoing (and might take years).[14]

Already during the Facebook investigation and after the decision of the FCO a large number of papers has been published with a wide range of critical and supportive opinions both on the case itself but often also about the wider implications of this case for the relationship between competition law and data protection / privacy law.[15] There are a number of critical points from a legal and economic perspective that we cannot discuss here, but we want to mention at least a few briefly. There is a broad consensus that it is a problem that the case is based upon German competition law, which - even if this decision stands - does not allow clear conclusions about the applicability of this approach according to the much more important Art. 102 TFEU in EU competition law.[16] There is also some critical discussion about the market definition and the dominance of Facebook,[17] but most commentators of the case (and also the courts) have accepted that Facebook is dominant on the German market for social media. There are critics who question whether this data-collecting behaviour of Facebook is a problem at all, i.e. whether it leads to any harm to consumers (also due to efficiency effects), and/or can have negative effects on competition, both in a general way and with respect to the specific Facebook case.[18] Most of the contributions about the Facebook decision, however, agree that this bundling behaviour of Facebook can be a problem and that there might be serious negative effects on privacy and/or competition. However a large part of the discussion is not about the problem whether such negative effects exist or not, but whether it is a task of competition law to deal with this data-collecting behaviour of large digital platforms also with respect to its effects on privacy,

---

11 See Bundeskartellamt (2019b, 5-6), and, e.g., also ACCC (2019, 22-23) for such concerns of a lack of “genuine choice".

12 See OLG Düsseldorf (2019).

13 See Bundesgerichtshof (2020)

14 See, e.g., Witt (2020, 32-35), Podszun (2020, 1276).

15 See, e.g., Schneider (2018), Volmar/Helmdach (2018), Colangelo/Maggiolino (2018, 2019), Botta/Wiedemann (2019), Haucap (2019), Këllezi (2019), Körber (2019), Budzinski et al. (2020), Buiten (2020), Witt (2020), Podszun (2020).

16 Most legal scholars that welcome the Facebook decision think that the behaviour of Facebook could also be seen as a violation of Art. 102 TFEU. See, e.g., Schneider (2018), Botta/Wiedemann (2019), Robertson (2020), Witt (2020).

17 See, e.g., Körber (2019), Haucap (2019).

18 See, e.g., OLG Düsseldorf (2019), Körber (2019).

and what it implies for the relationship between competition and data protection law. Since this is also our main research question, we will summarise the most important positions in this discussion regarding this question.

The main group of critics of the Facebook case defends the traditional approach of a strict separation of competition law and data protection law. From that perspective competition law might be capable of assessing data-collecting behavior of firms but only with respect to its effects on competition. Any privacy concerns through mergers or a behaviour of dominant firms are beyond the scope of competition law and should be dealt with by data protection law (and data protection authorities). Any intermingling of privacy protection with the protection of competition can lead to huge problems and endanger the clarity of competition law. This is the opinion of many competition scholars and the official position in many competition law regimes, as, e.g. in the U.S. and in EU competition law.[19] Many supporters of such a position however would not deny that this data-collecting behavior of large digital platforms might be a big problem for privacy that should be solved, but they claim that this should be left entirely to data protection or consumer law, because it is the market failure information and behavioral problems that causes this problem.[20]

Against this main counterposition to the Facebook decision of the FCO several other positions exist in the discussion, which all demand a more open application of competition law with regard to privacy effects.[21] Close to the traditional competition law approach are scholars who think it is possible to take into account privacy effects also in competition law, because privacy can be seen as part of consumer welfare (e.g. as part of the quality of a service). Rather uncontroversial is the position that also exclusionary effects of such a bundling behaviour of Facebook can have negative effects on privacy, e.g. through less competition on the market for social media itself or on other markets. Most of the contributions however focus on direct exploitative effects, i.e. that the terms of service of data-collecting practices might be assessed with regard to "excessive data collection" (in analogy to excessive prices) or "unfair business terms" as exploitative abuse of a dominant firm (e.g., in the EU Art. 102 TFEU). These approaches still use the well-established (but rarely used) approach of exploitative abuse, and also acknowledge the problems of determining a proper benchmark for qualifying a data-collecting behaviour as abusive.[22] One additional and new option for

---

[19] See, e.g., Körber (2019), Këllezi (2019), Buiten (2020); this is also the position of the EU Commission (see references in fn.10), and the main position in the U.S. (e.g., Ohlhausen/Okuliar 2015, Manne/Sperry 2015, Sokol/Comerford 2016, and, most recently, United States 2020). It should however be kept in mind that in the U.S. a very different approach to privacy prevails, and US antitrust law does not address exploitative abusive behaviour.

[20] See, e.g., Buiten (2020), and the EU Commission (see European Union 2020, paras. 29-42).

[21] For the distinction between two positions that either emphasize the separation or a more integrated approach regarding the relationship between competition and data protection law see Stojanovic (2020, 532) and Binns/Bietti (2020, 6). In the following, we also want to focus on a stronger differentiation of reasonings within the second group.

[22] See, e.g., Robertson (2020, 172-183), Colangelo/Maggiolino (2019, 369-371), Botta/Wiedemann (2019, 429).

solving this benchmark problem about abusive behavior is to use either data protection law or the fundamental value of privacy (on which the GDPR is based) for helping to decide whether the behaviour of a dominant firm is still acceptable or abusive with respect to its effects on privacy.

The FCO has in its Facebook decision directly used such a violation of EU data protection law as benchmark for exploitative abuse. A number of competition law scholars support this approach of the FCO, and see also possibilities to apply it not only in German but also in EU competition law (Art. 102 TFEU).[23] Particularly important is that also data protection authorities have supported such an approach, which also implies that they do not resent the activities of competition authorities with regard to privacy protection, but, on the contrary, support them.[24] This direct use of data protection law in a competition law proceeding has however provoked much critique. Beyond concerns about the capabilities of competition authorities to make data protection assessments, and potential conflicts between both laws, it was particularly criticized that using violations of the GDPR as benchmark in competition law would turn competition authorities into enforcement agencies for data protection law, with the possibility that any infringement of data protection law of dominant firms might be automatically seen as abusive in competition law.[25]

The main question about using violations of data protection law in reasonings about abusive behaviour is whether such a violation automatically leads to the abusive character of the behaviour or whether such a violation can be one factor within a much more comprehensive reasoning about balancing interests between the dominant firm and the consumers. The latter is a much more flexible and moderate position, which can be close to the above-described traditional assessment approach of exploitative abuse. The other option is to take into account privacy as a fundamental value in the reasoning about balancing of interests for determining abuse.[26] The recent Facebook decision of the German Federal Court of Justice, which supported the FCO, can be seen as being close to such a position (although it is based upon German instead of EU law). The court argues that the terms of Facebook, which do not allow users to choose between a more or less personalized service (through forcing them to consent to the merging of both sets of data), violate the "basic right" of informational self-determination of German consumers, which is protected by the German constitution. It then uses this as argument for qualifying this requirement as "abusive" in competition law (without refering to a violation of EU data protection law).[27] A very interesting question is whether such a reasoning with privacy as a fundamental value can also be used in EU competition law (e.g. in Art. 102 TFEU). In chapters 5 and 6 we will see how the new proposal of the Digital Market Act relates to this discussion, because it entails a

---

[23] See, e.g., Schneider (2018), Volmar/Helmdach (2018), and also Costa-Cabral/Lynskey (2017, 30-38).

[24] See Buttarelli (2019).

[25] See, in particular, the critique of Colangelo/Maggiolino (2019, 376).

[26] This approach does not raise serious problems for all those competition law scholars who are open to consider also other objectives (beyond competition / consumer welfare) in competition law. See, e.g., with respect to data protection and privacy, Costa-Cabral/Lynskey (2017).

[27] See Bundesgerichtshof (2020); see with regard to this decision also Podszun (2020).

far-reaching ex-ante prohibition of such "bundling of consent" requirements for personal data for all gatekeeper platforms.

Additionally, also a number of contributions can be found that welcome the Facebook case and its discussion, because it opens a much broader discussion about the need to develop a broader policy perspective on the manifold, complex, and interlinked problems of the data economy, in which market power problems of large digital platform firms (with gatekeeper positions), data concentration, and unsolved privacy problems of consumers through intransparency and "dark patterns" behaviour etc. might be directly intertwined with each other. These contributions see the necessity to overcome the narrow traditional approaches of competition law, data protection law, and others, and suggest the development of new and more integrated policy approaches (including collaboration between the enforcement agencies of different policies).[28]

This international discussion about the Facebook case of the German FCO has shown a broad range of positions. They all deal with the question whether and how competition law can take into account data-collecting practices and privacy terms (esp. this "bundling of consent") of a dominant digital platform firm like Facebook with respect to competition and privacy, and what the role of data protection law can be regarding these problems. In the following chapter 3 we are analyzing from an economic perspective, whether the main counterargument to the Facebook case, i.e. the thesis of a strict separation of competition and data protection law, can be defended in cases like the Facebook case. In these cases we have - as most of the scholars in this discussion would agree - a situation with the simultaneous existence of two market failures, namely (1) a competition problem (here: market dominance), and (2) an unsolved information and behavioral problem of consumers. What implications follow from such an analysis for the relationship between competition law and data protection law? This is a question that so far has not been analysed in a systematic way.

3. Competition policy and privacy protection: Two market failures, two policies, and their interaction

From an economic perspective different policies should fulfill different tasks, i.e. solving different market failure problems and/or achieving different policy objectives. Whereas competition policy should solve market failures through competition problems, data protection (or privacy) policies have the task of protecting the privacy of individual persons (and their informational self-determination). If we interpret the EU data protection law (GDPR) from an economic perspective, then it focusses on the solution of two different problems: On the one hand, it defines and assigns a bundle of rights on personal data to individual persons, and, on the other hand, it helps solving information asymmetry and behavioral problems of these persons with regard to contracts that allow other firms to process, collect, and use their personal data. Since consumer policy also intends to solve this type of market failure, the GDPR can also be interpreted as a specific consumer policy with respect to personal data.[29] Since in the EU the

---

[28] See, e.g., Costa-Cabral/Lynskey (2017), Binns/Bietti (2020), Kemp (2020).

[29] For analyses of the similarities and differences between competition law, data protection law and consumer law in the EU, see from a legal perspective, in particular, Costa-Cabral/Lynskey (2017), as well as Graef/Clifford/Valcke (2018),

GDPR protects privacy also as a fundamental value, this additional normative objective can lead to trade-off problems with the objective of economic efficiency.[30] In the following, we narrow down the analysis by focussing only on the two market failures competition problems and information / behavioral problems of consumers,[31] and analyze from an economic perspective the relationship between these two policies in situations of a simultaneous existence of both market failures as in cases like the Facebook case.

The established standard approach both in the law and in economics is that we analyze and remedy a certain market failure problem separately, and usually under the implicit assumption that it is the only market failure on this market. If we have, for example, a competition problem through a dominant firm, we only look at the competition problems, and do not take into account whether there are at the same time also information asymmetry problems on these markets. In the same way, also data protection law (or consumer law) does not take into account whether a firm is dominant or not when trying to solve market failure problems through information or behavioral problems of consumers. Therefore the main critique of the Facebook decision of the FCO is entirely in line with this standard approach: Competition law should deal with the competition problems, and data protection/consumer law with the information/behavioral problems. However, the policy discussions about large digital platform firms have already shown very well that in the digital economy these two market failures might be deeply intertwined, suggesting that such a separation approach might not work any more, and a more complex approach is necessary. From the perspective of economic theory this is not surprising, because this standard approach of a separate application of different policies is based upon a number of assumptions,[32] which need not be fulfilled under the real-world conditions of the digital economy.

The main problem is that this standard approach can only work, if (1) the effects of the two market failures, and also (2) the effects of both policies (including remedies) are independent from each other. This assumes that competition problems, as, e.g., cartels, mergers, and dominant firms, have no impact on (the effects of) the information and behavioral market failure, as well as, vice versa, the latter market failure has no impact on competition problems. A similar problem of interaction effects also emerges at the policy level. Here the standard approach would also assume that the effects of one policy (as, e.g., competition law with respect to its effects on competition) do not depend on the application of the other policy (as, e.g., data protection / consumer law), i.e. how the other policy tries to solve the second market failure and how successful it is in that respect.

Botta/Wiedemann (2019), Graef/van Berlo (2020), and from an economic perspective Kerber (2016).

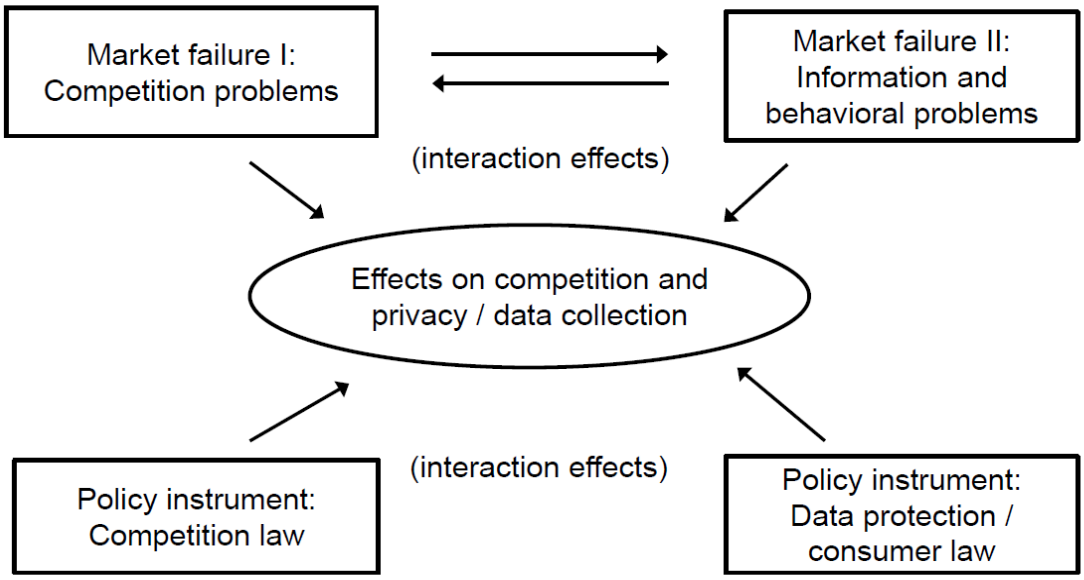
30 Kerber (2016, 645).

31 It is not possible here to discuss, to what extent also additional market failures might be relevant here, as, e.g., "missing markets" for personal data (Economides/Lianos 2021), or "data externalities" that lead to excessive data-sharing (Acemoglu et al 2020).

32 It is wellknown in economics for a long time that policies that intend to reduce one market failure might fail (and even worsen the situation), if at the same time a second (unsolved) market failure exists. In welfare-theoretic microeconomics this problem has been analyzed in the "theory of the second-best" (Lipsey/Lancaster 1956).

The following Figure 1 illustrates this problem. These interaction effects can exist both between the market failures themselves and their effects on competition and privacy, but they can also exist in that way that the application of competition law (data protection law) can have effects on privacy (on competition). The latter also implies that the aggregate effects of both policies on competition and privacy can depend on the specific combination of both policies (and their remedies). If such interaction effects between these two market failures and two policies exist, then it can be concluded from an economic perspective that any separate application of both policies that ignores these interaction effects can lead to suboptimal policy decisions, suggesting the need for a coordination of both policies. Whether and to what extent such interaction effects exist, is an empirical question. In the following, we will briefly show that many of these interaction effects have already been an issue in the current policy discussions.

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



The information and behavioral problems of consumers regarding their consent to contracts with data-collecting firms about the collection and use of personal data and the ensuing problems for the "notice and consent" solutions are well-researched and broadly accepted as a largely unsolved market failure problem in the discussion. Due to intransparency and also misleading practices of data-collecting firms consumers are overwhelmed and cannot compare different privacy policies of firms, which - according to a wide-spread opinion - is also the reason, why competition with privacy-friendly terms and conditions does not work in an effective way.[33] So far the attempts to improve this competition through more efforts for transparency have proven futile.[34] This market failure also leads to an entry barrier for firms that would like to offer more privacy-friendly services to respond to heterogeneous privacy preferences. It also makes it easier for the large digital platform firms like Facebook to collect large quantities of

[33] For the problems of "notice and consent", privacy paradox, "dark patterns" and "concealed data practices" see, e.g., Solove (2013), Acquisti et al (2016, 479), Kokolakis (2017), Waldman (2020) and Kemp (2020).

[34] As possible future instrument privacy icons, privacy certification, or standardisation of privacy policies are discussed.

personal data, which strengthens their competitive advantages on a multitude of markets. These are some of the already well-discussed effects of information and behavioral problems on competition.[35]

What about the effects of competition problems on information and behavioral problems and privacy? Less competition, e.g. through the existence of a dominant firm, a cartel about data-collecting (or data-sharing) practices or large lock-in effects of consumers, can lead to less choice for consumers between different services with different data-collection / privacy protection levels. This can lead to lower incentives for consumers to invest in screening of privacy policies, which aggravates the information problems. At the same time, dominant firms can use less transparent and more misleading behavioral targeting practices to get consent to more far-reaching data-collecting privacy policies, because consumers cannot avoid these firms.[36] Therefore the question emerges whether competition problems, and information and behavioral problems might reinforce themselves mutually, and lead to the resignation of many consumers, because they realize that they have no realistic chance in controlling their data and protecting their privacy.[37]

There are also well-established discussions about interaction effects at the policy level. One important discussion focuses on the question whether data protection law itself, especially the strict data protection law in the EU, can have negative effects on competition. In that respect it is claimed that the GDPR with its high requirements for consent supports the concentration of personal data on a few large digital platform firms, strengthens their competitive advantages and increases entry barriers.[38] However, it is also widely assumed that data portability rights (like Art. 20 GDPR in the EU) can also help to enable more competition (by reducing switching costs and lock-in problems), leading to the current discussion about making this data portability right more effective.[39] Again, it can be asked, vice versa, about the effects of competition law on privacy. Can the prohibition of cartels, merger control, or the prohibition of abusive behavior of dominant firms have positive effects on privacy? Theoretically economists would assume that in a well-functioning market, i.e. without information and behavioral

---

35 See also the concept of intermediation power in Schweitzer et al. (2018, 85-100). Here it is argued that the fact that large digital platforms are also information intermediaries (with information asymmetries vis-a-vis consumers) implies that they also have an information manipulation power, e.g. through biased rankings and ratings, with which they can influence the behaviour of consumers, and, thus, increase their market power (see also Crémer et al. 2019, 49).

36 The huge amount of personal data large digital platforms already have on many consumers, also allows them not only to use much more effective targeted behavioral strategies to nudge consumers to give more personal data, but also to use “dark patterns” and more deceptive strategies (see Forbrukerradet 2018, Srinivasan 2019, 92-97).

37 See Turow et al. (2015), Condorelli/Padilla (2020, 44).

38 See, e.g. Campbell et al. (2015), OECD (2020, paras. 162-169), Gal/Aviv (2020), Johnson et al. (2021)

39 See, e.g., Krämer et al (2020). However there are also concerns that the data portability right might also strengthen the market power of the large digital platform firms (see, e.g., de la Mano & Padilla 2018 with respect to the effects of the Second Payment Service Directive).

problems, effective competition would lead in the same way to a better fulfillment of privacy preferences as with regard to other preferences. Empirical studies about the effects of competition on privacy, which so far have led to inconclusive results, suffer from the problem of the simultaneous existence of both market failures.[40] However, also negative effects of competition law on privacy are being discussed, especially with respect to remedies that would try to improve competition through requiring the sharing of personal data, e.g. of large digital platform firms with other smaller competitors.[41]

It is not possible here to analyze these interaction effects in more detail or to give a comprehensive overview about the results of the already existing research. But these discussions show the empirical relevance of these interaction effects, especially with respect to the data-collecting behavior of digital platform firms. From an economic policy perspective this leads to the conclusion that a separate application of both policies, which would ignore the other market failure and policy and these interaction effects, would lead to suboptimal decisions in both policies.[42] A wellknown example is the critique of the approach of the EU Commission in its assessment of data mergers, which surprisingly assumed that competition law need not take into account the effects of the mergers on privacy, because data protection law would solve any privacy problems through the combination of the merging firms' data sets.[43] As a consequence, the standard approach of a strict separation and simple division of labour between competition law (solving competition problems) and data protection law (solving privacy problems) does not fit for the digital economy, and a more complex and sophisticated relationship between both policies that takes into account these interaction effects is necessary.

In the following chapters, we will apply this theoretical framework of two market failures, two policies, and their interaction effects to the question whether (and how) competition law can take into account negative effects of competition problems on privacy, as they have been claimed in the Facebook case. In the next chapter 4 we will ask whether competition law and/or data protection law can deal with such negative effects of competition problems on privacy. After coming to the conclusion that only competition law can help in that respect, we will analyse in a much deeper way in chapter 5, how the control of abusive behavior of dominant firms can be applied for dealing with the exclusionary and exploitative effects of data-collection / privacy terms behavior in cases like the Facebook case of the FCO.

---

[40] See Blankertz (2020) for an overview of these empirical studies and the mechanisms of effects of competition on data-collection and privacy. See also Esayas (2018, 183-192) for a broad discussion of market structure and data privacy that includes also behavioural aspects. Here much more research is necessary.

[41] See for this problem, e.g., Crémer et al (2019, 104), and, in the U.S. discussion, Douglas (2020).

[42] See also Jin/Wagman (2020, 20).

[43] See OECD (2020, paras. 69-73), where it it criticized that the EU Commission in its application of competition law has assumed erroneously in many competition cases (with potential effects on data and privacy) that the GDPR is solving the privacy problems, and that therefore the EU competition policy can ignore these effects. See more generally also Lynskey (2018).

4. Negative effects of competition problems on privacy: A task for competition or data protection law?

4.1 Competition law

The question that we want to answer here is whether, in general, data-collection behaviour (and, e.g., the specific "bundling of consent" in the privacy terms) of digital firms can be taken into account in competition law. It is clear that there is no problem of applying competition law to such practices, if there are direct negative effects on competition. If firms collude on the extent and conditions on data collection, e.g. through agreements on their privacy policies, then such behavior can infringe competition law provisions against cartels (as Art. 101 TFEU in the EU). Also the combination of data sets can raise problems in merger reviews, if it can impede competition on a market, e.g. through erecting barriers to entry. In the same way, also a certain data-collection behavior of a dominant firm can be prohibited as abusive (Art. 102 TFEU), if this behavior has exclusionary effects and therefore impedes competition. The interesting question is whether competition law can also take into account the negative effects of such a behaviour on the privacy of consumers.

If we start from an economic perspective with the consumer welfare standard in competition law, then it is no problem to take into account in competition law all negative effects on privacy, as long as they can be interpreted also a reduction of consumer welfare. This is also the reason why economists have no problem to agree to the widely-held view that privacy can be seen as part of the "quality" of a service.[44] The relationship between the data-collecting behaviour and privacy policies of digital firms and consumer welfare is however a complex one that needs careful consideration (and, in fact, much more research). It is often claimed that market dominance can lead to excessive collection of data in direct analogy to excessive prices. The wide-spread interpretation of data as a counterperformance for “free” services also suggests that the harm to consumers is that they have to pay a too high “data price” for these services. However, due to the non-rivalrous character of data the consumers do not have less personal data than without the data-collection (and retain the right to share these data with others).[45] Therefore the direct analogy to excessive prices is problematic with respect to effects on consumer welfare: In contrast to a higher monetary price the collection of more data, e.g. through such a bundling of consent as in the Facebook case, need not always lead to less consumer welfare.[46] Nevertheless it is still possible that such a behaviour can be qualified as "excessive data collection", but a more sophisticated reasoning is necessary. We cannot discuss here in detail, under what conditions and how the collection of more personal data (and/or a broader use / sharing of these data through far-reaching terms in the privacy policies) can lead to more harm

---

[44] See, e.g., Stucke (2018, 285-290), Lynskey (2018), Esayas (2017).

[45] Important is also that, economically, personal data are not "sold" but "licensed" to data-collecting firms. Since this is a non-exclusive licence, consumers retain the right to allow also other firms to use these data.

[46] See, e.g., Haucap (2019, 2-3). In addition, providing more data allows for more personalised services, which also can increase consumer welfare.

to consumers.[47] In the following, we will focus only on two economic reasonings: Privacy risks and privacy preferences.[48]

It was always a main argument in data protection law that the collection of more personal data (or a wider use/sharing of data) can lead to higher privacy risks. These are the additional risks that consumers have to bear, because these data, which can be combined with many other data to comprehensive consumer profiles, can be used for business practices (or other behaviour) that can harm them in the future (behavioral targeting, fraud/extortion, price discrimination etc.). Therefore, revealing more personal data can lead to higher objective risks for consumers about getting harmed, and it is clear from an economic perspective that these risks reduce consumer welfare.[49] Since one of the huge problems is that consumers usually cannot assess these privacy risks, it is hard or impossible for them to make well-informed and rational decisions whether very short-term benefits for providing their data are worthwhile enough for bearing these risks in the near or far future.[50] If through competition problems (like cartels, mergers and dominant firms) consumers have to accept the collection and far-reaching use of more personal data, then these larger privacy risks decrease their consumer welfare, and are therefore relevant for competition law.

Consumer welfare also depends on the fulfillment of privacy preferences. We know from empirical studies that consumers have very heterogeneous preferences about whether and to what extent which kinds of personal data they would like to reveal under what circumstances to which firms (or other organizations) and for which purposes.[51] In a well-functioning market we would assume that a broad range of firms exists with different privacy policies, i.e. there would be firms that offer services with high privacy standards (and only a low level of data collection), and others with "free" services and a low level of privacy protection (and large collection of data). Depending on the extent of data collection also different monetary prices might have to be paid for these services. It can also be expected that the same firms offer their services with different privacy options (with and without data collection) and prices, from which their customers can choose. In such a well-functioning market, with a wide range of options for making granular decisions about making personal data available to certain firms and for certain purposes, consumers could choose services with those privacy policies that fit best to their preferences, and also optimize their decisions about benefits and risks of revealing personal information. Being capable of making such choices would increase the welfare of the consumers. This implies that the non-existence of such a range of options for choosing the optimal privacy solutions, e.g., through such an

---

[47] See for various overviews about this discussion with many references, e.g., Esayas (2017), Colangelo/Maggiolino (2018, 232-235), OECD (2020, 25-32).

[48] We are particularly not discussing the important question, whether competition problems lead to lower "prices" that consumers can get for their personal data as a reasoning for "data exploitation".

[49] The principles of data minimization and limiting consent to specific purposes in data protection law can be understood as principles of caution that help to limit these privacy risks.

[50] See, e.g., Solove (2013).

[51] See Acquisti et al. (2016, 444-448) and Kerber (2016, 642) with further references. Also the FCO used such a survey in its Facebook decision (Bundeskartellamt, 2019a, 5-6).

uniform take-it-or-leave-it "bundling of consent" by a dominant firm (as in the Facebook case), will have negative effects on consumer welfare (particularly for consumers with strong privacy preferences). Therefore having not enough choice for consumers can also be seen as reducing consumer welfare.[52]

Our preliminary result is that negative effects of competition problems on privacy, e.g. through cartels, mergers, or abusive behavior of dominant firms, can be taken into account in competition law, because the increasing of objective privacy risks and the non-fulfillment of heterogeneous privacy preferences through excessive collection of data and/or excessive terms can be interpreted as directly reducing consumer welfare. In that respect, privacy can be seen as part of the non-price parameter quality, or even as a separate non-price parameter. If therefore competition problems, as, e.g., horizontal agreements about privacy policies or the behavior of dominant firms, have negative effects on the privacy of consumers, then this is also a genuine concern for competition policy in a similar way as higher prices or less innovation.

4.2 Data protection law

Can also data protection law deal with those negative effects of competition problems on privacy? In the following, we will present two arguments, why data protection law is generally not capable of solving these problems.

First, there is a broad consensus that EU data protection law establishes minimum standards for privacy protection. It is however expected that on well-functioning markets also higher levels of data protection than this minimum standard would be offered.[53] This implies that any negative effects of competition problems on privacy, e.g. with respect to larger privacy risks due to excessive collection and use of personal data through firms with market power (or through a cartel or a merger), cannot be dealt with by the GDPR, as long as these firms still comply with these minimum standards. The decisive point is that competition law also protects competition with data-collecting behaviour and privacy terms, and therefore also privacy levels above these minimum standards against anticompetitive behaviour and competition problems. This is also the reason why, in general, compliance with the GDPR does not shield firms from competition law violations with regard to their data-collecting behaviour and privacy policies.[54]

The second problem is that EU data protection law focuses on protecting consumers with respect to a different market failure, namely information and behavioral problems of consumers with regard to the contractual arrangements about collecting and use of personal data. In that respect both data protection law and consumer law can be applied.[55] In data protection law this leads, inter alia, to the requirements for a valid consent, and the already mentioned very critical discussion about the effectiveness of

---

[52] In the legal discussion consumer choice has always been seen as an assessment criterion in competition law (see, e.g., Averitt/Lande 2007).

[53] See on competition on data protection conditions also Costa-Cabral/Lynskey (2017, 20) and Esayas (2018)

[54] See also Robertson (2020, 177).

[55] See Kerber (2016, 645), Costa-Cabral/Lynskey (2017), Botta/Wiedemann (2019).

"notice and consent" solutions for making well-informed and rational decisions with respect to personal data.[56] It is this focus on the market failure "information and behavioral problems" which makes data protection law incapable of dealing with negative effects of competition problems on privacy. Both the legal provisions of data protection law and also the tool-box of data protection authorities do not allow the analysis of competition problems and their solution through appropriate remedies. Since it is a very important principle in EU data protection law (and in other privacy laws) that all firms are treated equally with respect to their data-collection and privacy terms, data protection law cannot distinguish between firms with and without market power.[57] It is not possible that the privacy policies of firms that are not under effective competition (dominance, horizontal agreements) are assessed more critically than those of firms under effective competition, implying that the different effects on privacy between these different groups of firms cannot be considered. Therefore competition and market power are not criteria for assessing the compliance with the GDPR.

Particularly among competition lawyers there is a discussion whether market dominance might also be taken into account in the GDPR as part of the assessment of the requirements for a valid consent (Art. 4(11) GDPR). The argument is that in the case of a dominant firm the consumers might not have the possibility of providing a "freely given" consent any more, which might render their consent invalid.[58] It can find limited support in the Art. 29 Data Protection Working Party Opinion about legitimate interests of data controllers, in which also the dominant position of a company on the market is briefly mentioned as one of the factors that can be considered.[59] However, the principle of treating all kinds of firms equally with respect to data-collection and privacy terms is, so far, deeply entrenched in the practice and jurisprudence of EU data protection law.[60] Since, however, EU data protection law uses a risk-based approach with regard to privacy protection, treating firms differently according to different privacy risks linked to different types of firms would be compatible with such an approach. If the data-collecting behaviour and privacy terms of dominant firms lead to larger privacy risks than those of non-dominant firms, then such a differentiation might be appropriate also from an economic perspective. It is however less clear whether in data protection law such a risk-based rationale for differentiating between different types of firms regarding data collection and privacy terms would see market power or lack of effective competition as the main criterion for such a differentiation, or only as one of a number of criteria.[61] But even if market power can be established as such a criterion, then there

---

[56] See the references in fn.33.

[57] See Colangelo/Maggiolino (2019, 366), Botta/Wiedemann (2019, 445), Lynskey (2019, 203).

[58] See the discussion in Botta/Wiedemann (2019, 439). The FCO in its Facebook decision has also used this argument (Bundeskartellamt 2019a, 11-12).

[59] See Art. 29 Data Protection Working Party (2014, 40).

[60] This is also the reason why it was criticized that the FCO with its Facebook decision would extend the data protection requirements for dominant firms. See Colangelo/Maggiolino (2019, 366), Këllezi (2019, 355-356) but also Crémer et al. (2019, 80).

[61] See Graef/Van Berlo (2020), who propose to use the "special responsibility" principle of Art. 102 TFEU also in EU data protection law, which would enable to treat dominant and non-dominant firms differently. Another approach has been suggested by Lynskey (2019), who introduces a much broader concept of "data power" of digital

is still the problem of the lacking expertise and remedies of data protection authorities for analyzing competition problems and implementing appropriate remedies. In any case, however, these questions should be on the agenda for future reform discussions in data protection law as well as for a possible collaboration with competition authorities (see chapter 6).

This section has shown that data protection law is not capable of dealing with negative effects of competition problems on privacy, because it only protects a minimum standard of privacy protection and focusses with its instruments on a different market failure. Consumer law as another policy instrument that can be applied to data-collection and privacy policies of firms runs into the same problems. It can help to deal with issues of transparency and misleading terms and conditions, but it also cannot treat firms with and without market power differently or even deal with negative privacy effects of mergers and cartels. In that respect, it is important that the Italian competition and consumer protection authority AGCM in 2018 imposed a fine on Facebook for misleading consumers and aggressive commercial practices as violations of Italian consumer law (codice del consumo), which implements the EU Unfair Commercial Practices Directive. The allegations refer to the practice of misleading consumers that the service is "free" despite that it has to be paid with personal data, and to practices that discourage users from blocking the transfer of their personal data to other websites.[62] However the Italian Facebook case also clearly shows that consumer law has to frame the problem as an information or behavioral problem, which usually does not fit to the competition problem.[63]

The result of our analysis in this section is therefore that competition law can and should take into account the negative effects of competition problems on privacy, because data protection law and consumer law is not capable of dealing with these negative effects on privacy.[64]

5. Assessing the abusive behavior of dominant firms with regard to data-collection behaviour and privacy terms

5.1 Introduction

Since data protection (and consumer) law cannot deal with negative effects of competition problems on privacy, the main counterargument against the Facebook case of the FCO that effects of competition problems on privacy is outside of the scope of

platforms, which includes also other types of data power than only market power, and then discusses different options how to deal with such firms with data power. Both proposals are based upon the risk-based approach of the GDPR.

[62] See Botta/Wiedemann (2019, 442-444).

[63] An additional problem is that due to the impossibility of taking into account market dominance in consumer law, a danger of over-regulation arises, because the prohibition of certain practices of data-collection and privacy terms would then also apply to non-dominant firms, whose use of these practices might be unproblematic.

[64] An additional problem of EU data protection law is that it has a serious enforcement deficit (partly due to under-staffed data protection authorities). See as overview Lancieri (2021).

competition law cannot be defended. On the contrary, only competition law is capable of dealing with these effects. After having clarified that the data-collecting behaviour and privacy terms of Facebook can be relevant in competition law, this chapter will discuss in more detail how it can be assessed within the control of abusive behaviour of dominant firms in EU competition law (Art. 102 TFEU). This will be done in close connection with the Facebook case and its controversial discussion, including the most recent developments in courts as well as the surprising inclusion of this issue in the current proposal of the Digital Market Act.

5.2 Exclusionary abuse

In the Facebook decision, the FCO has primarily focussed on assessing whether this "bundling of consent" in the terms of service can be qualified as an exploitative abuse, and only very briefly whether it also can have exclusionary effects. The FCO argued that through the violation of the GDPR Facebook was capable of getting an unlawful competitive advantage, which would lead to impeding its competitors. It can increase entry barriers and enable Facebook to defend its dominant position not only on the market for social media but also on advertising markets.[65] The critical discussion focussed on the problem that the FCO did not try to substantiate this claim through a deeper investigation or the provision of evidence how the additional data would impede competition or raise entry barriers.[66] It was widely regretted that the FCO has not used more the opportunity to investigate the potential exclusionary effects both on the market for social media and on other markets, especially the advertising markets, because this would have allowed for a much less controversial reasoning regarding the abusive character of this "bundling of consent" requirement of Facebook. However, it has to be considered that we have gotten only very recently more insights into the working of digital advertising markets and the critical role of Facebook and Google in this sector. Therefore it might have been very difficult for the FCO to provide sufficient evidence about such exclusionary effects at the time of its decision.

In the meantime, a number of recent studies have shown that Google and Facebook are dominating a very complex structured advertising industry with serious competition problems and inefficiencies. According to the comprehensive CMA report (July 2020) Google is dominant on the market for search advertising, whereas Facebook has market dominance on the market for display advertising.[67] There is considerable empirical evidence that both Google and Facebook have huge advantages through their superior access to first- and third-party data about consumers in targeting consumers. Since Facebook is not only dominant on the market for social media, but is assessed by the CMA even as a "must-have" platform for consumers, the latter have no real choice by switching to other competitors and have to accept also unfavourable data policies. Therefore Facebook's dominant position cannot be challenged by competition. Based upon this and other research, it is now much easier to show that such a "bundling of consent" can have exclusionary effects and therefore can be seen as an abusive

---

65 Bundeskartellamt (2019a, 13)

66 See, e.g., the critique of lacking evidence in the decision of the OLG Düsseldorf (2019, 32-36)

67 CMA (2020a, paras. 3.189-3.157); the Australian ACCC report (2019, ch. 2.6, 2.7) came to the same conclusion for the Australian markets for digital advertising.

behaviour.[68] Both the decision of the German Federal Court of Justice as well as the proposed Digital Market Act emphasizes the importance of such exclusionary effects.[69]

5.3 Exploitative abuse

Both in competition law and in competition economics there was always a controversial discussion about the control of exploitative abuse of dominant firms, and competition law regimes in the world differ about whether to control exploitative abusive behavior of firms with market power. Both in the EU and some Member States, as, e.g., Germany, the control of exploitative abuse is an integral part of the control of dominant firms. If competition policy - in accordance with the consumer welfare standard - is understood also as an instrument for protecting consumers against welfare losses through the abuse of market power and anticompetitive behavior (as, e.g. price cartels), then controlling the behavior of dominant firms with respect to exploitative abuse of consumers is an essential pillar of competition policy.[70] The reluctance of competition authorities to apply this instrument of exploitative abuse, and also the skeptical attitude of competition scholars, who see it only as an instrument in exceptional cases, has its cause in the difficulties of its practical application. This refers to the question how to determine what an abusive price is, and the understandable fear of competition authorities to evolve into price-control authorities. This reluctance with regard to price abuse is to a large extent justified,[71] but it is no general argument against the use of the instrument of controlling exploitative abuse. However, it does emphasize the importance of the criteria for determining an exploitative abuse and the potential need to limit its application to particularly serious problems of exploitative abuse. This is also important with respect to the collection of personal data and harm to privacy by dominant firms.

In cases of exploitative price abuse the usual approach from an economic perspective is to compare the actual price with a benchmark price under competition (price on another market with effective competition, analysis of costs etc.).[72] Due to the characteristics of (multi-sided) platform markets (with its network externalities, tendency to tipping, and complex pricing behaviour) such an approach to price abuse is much more difficult on platform markets than on markets for normal products and services.[73] In addition, we already have seen (in section 4.1) the difficulties of a direct transfer of the concept of excessive pricing to excessive data-collection. An additional problem is that

---

[68] See also Condorelli/Padilla (2020) about envelopment strategies through "tying of privacy policies".

[69] See Bundesgerichtshof (2020, 37), Draft DMA (recital 36) (European Commission 2020a), and below section 5.4.

[70] Therefore competition policy does not protect only competition, but also consumers against the redistributive effects of market power and anticompetitive behaviour. See for this discussion Kerber (2009, 101-104).

[71] See for a summary of the current view on exploitative price abuse in EU competition law Ayata (2020).

[72] See from an economic perspective, e.g., Bishop/Walker (2010, 237-244).

[73] See Ayata (2020).

the negative effects on privacy (e.g. privacy risks like data breaches) might be much larger, if the same behaviour is applied by a dominant firm than a non-dominant firm. Therefore using the direct analogous approach of comparing the data-collection (and privacy) terms of a dominant firm with those of firms under effective competition does not seem to be a feasible approach for solving the problem. However, from a legal perspective, it is not necessary, e.g. in the application of Art. 102 TFEU, to use such a counterfactual, and therefore also other reasonings for exploitative abuse are possible.

In the legal literature a broad discussion can be found about the possible criteria for assessing whether excessive data collection (and privacy terms) can be assessed either in analogy to "excessive prices" or as "unfair trading conditions".[74] It is not possible to discuss these criteria in detail, but competition lawyers see, in particular, reasonings about "unfair trading conditions" (Art. 102 (a) TFEU) as a possible way for determining an exploitative abuse with respect to excessive data collection.[75] Criteria for the assessment of the fairness, e.g., of such a behaviour as this "bundling of consent", can be the indispensability of this condition for Facebook's business model and its operational interest, the principles of equity and proportionality, the bargaining power between Facebook and the consumers, and the consideration of EU data protection rules and principles.[76] It is not possible here to analyse this legal approach of balancing interests with respect to fairness from an economic perspective. It is, however, important to note that the concept of fairness for controlling exploitative distributional effects through powerful firms has emerged recently as an influential new reasoning in the current competition policy discussion about large online gatekeeper platforms, as, e.g., in the Digital Market Act proposal of the EU Commission. However, it is difficult for competition economists to deal with fairness as a normative criterion. But economists would always recommend that also the effects of a behaviour, e.g. here the "bundling of consent" on Facebook, the consumers, and competition on the market for social media and other (e.g., digital advertising) markets should be analysed and included in such an assessment of fairness.

This emphasis of economists on the effects of a behaviour leads us to the need for a much deeper analysis and more research about the theories of privacy harms through data-collection behaviours and privacy terms. Commentators of the Facebook decision emphasized that the FCO did not develop a clear theory of harm but relied on (what lawyers call) "normative causality", i.e. that it used already existing legal assumptions about causal effects of market dominance in other legal rules for concluding negative effects on privacy instead of proving these effects on privacy in its own investigation.[77]

---

74 See, e.g. Robertson (2020, 172-183), Botta/Wiedemann (2019, 429).

75 See e.g., Robertson (2020, 183), Colangelo/Maggiolino (2019, 369-371).

76 For these criteria, see Robertson (2020, 183).

77 The concept of "normative causality" is difficult to understand for economists. See with respect to its application in the Facebook case Witt (2020, 38-41). Much more important is the discussion of the socalled "causality problem", i.e. whether it is necessary to show a causality (a) between the dominance and the negative effects of the abusive behaviour on competition or the consumers, i.e. "effects-based causality", or (b) between the dominance and the abusive conduct (here the abusive privacy terms), i.e. "conduct causality". From an economic perspective, which would look at the effects on competition and consumer welfare, "effects-based causality" is the appropriate concept. If both dominant and non-dominant firms use the same privacy

Although this might be sometimes a legitimate approach within the law, it would be very helpful, if we would have much clearer reasonings and evidence about the harm to privacy (and the welfare) of consumers. What is the harm to privacy (and welfare) of consumers, if a dominant firm like Facebook, which can perhaps not be avoided due to the "must have" character of its social media platform service, applies such a "bundling of consent" requirement? In section 4.1 we already discussed that such a requirement, for example, might lead to higher (objective) privacy risks (consumer profiling) and less fulfillment of heterogeneous privacy preferences, and therefore can have redistributional effects from the consumers to the firm with market dominance (here: Facebook).[78]

Therefore much more general research is necessary about all these (and other) theories of harm of data-collection behavior and privacy terms for consumers in situations with serious competition problems.[79] Such a research should not be primarily done by competition authorities (as part of their investigations) but by interdisciplinary academic research. It should also include (the second market failure) informational and behavioral problems, and not only focus on objective privacy risks and consumer welfare in the traditional sense but also on privacy as a fundamental value, on fairness, and, e.g., also on freedom of choice. The results of this interdisciplinary research can then also be used for developing clearer benchmarks about where is the line that separates abusive and non-abusive data-collecting behavior (and privacy terms) in cases of exploitative abuse by dominant firms (or, in the future, fair and unfair behavior of gatekeepers in the proposal of the Digital Market Act).

5.4 The solutions of the German FCO and Federal Court of Justice in the Facebook case and the EU Digital Market Act proposal

The most controversially discussed issue in the Facebook decision is the approach to use the infringement of EU data protection law as a benchmark for determining that this "bundling of consent" is an exploitative abuse in competition law. The FCO therefore did not use the traditional approaches of assessing excessive data-collection in analogy to price abuse or as "unfair business terms". Rather it made a deep assessment whether these terms of service of Facebook violate EU data protection law, and derived directly from such a violation their abusive character. This approach was heavily criticized in the discussion and led to the allegation that any breach of data protection law or other laws through dominant firms can be seen and sanctioned as an abusive behaviour in competition law. That raised concerns that competition authorities

---

terms, then it can still be abusive if these privacy terms have more negative effects if applied by a dominant instead of a non-dominant firm. These and other causality issues cannot be discussed here in detail.

78 It is also discussed that the exclusionary effects of these increased data advantages of Facebook (and Google) on digital advertising markets can lead to higher advertising prices and therefore higher prices for other products and services for consumers (CMA 2020a, 312-316).

79 However, our emphasis on the need for more research about privacy effects does not imply that it is necessary that these effects have to be proven in specific cases. From a law and economics ("error-costs") perspective these insights can also be used for introducing economically sound rules or (rebuttable) presumptions about these effects.

can develop into super enforcers.[80] In our view this approach of the FCO has led to a very unfortunate, misleading, and distracting general discussion whether any violation of other laws by a dominant firm can also be seen as an abusive behavior in competition law.

From our analysis of the problem of two market failures, two policies, and their interaction, it cannot be the task of competition law (and competition authorities) to enforce data protection law. In chapters 3 and 4 we already have seen the differences regarding the objectives and instruments of both policies. Even if we take into account in competition law the negative effects of competition problems on the privacy of consumers, as it is also intended in the Facebook case by the FCO, the infringement of data protection law is neither a sufficient nor a necessary condition for the abusive character of the behaviour of a dominant firm: In chapter 4 we have seen that competition law can protect the privacy of consumers to a larger extent than the minimum standards of data protection law. Vice versa, not every data protection violation of a dominant firm can be seen as an abusive behaviour in competition law.[81] This however does not preclude the possibility that under certain circumstances a specific infringement of the GDPR can be used in a more comprehensive assessment of the abusive character of terms of services, e.g., as part of an assessment of "unfair business terms". But this has to be assessed on a case-by-case basis. We therefore do not recommend the approach to directly derive the abusive character of certain terms of service from their violation of EU data protection law. This would not reflect the complexity of the relationship between both policies.

It can however be asked whether instead of EU data protection law also privacy as a fundamental value can be taken into account in such a broader assessment approach. This would imply that competition law can consider in certain (perhaps exceptional) cases also other fundamental rights in competition law decisions, as it has been suggested by competition lawyers.[82] Economists are usually very reluctant considering additional objectives of competition law but under certain circumstances this might be appropriate.

The solution of the German Federal Court of Justice in its decision in the interim proceedings of the Facebook case used such an approach, albeit not by refering to privacy as a fundamental value at the EU level but by taking into account the "basic right" of informational self-determination, which is protected by the German constitution. According to the court the right on informational self-determination grants individual persons the possibility to participate substantially and in a differentiated way whether and how its personal data are made available to others and can be used by others. The court argues that forcing the consumers through these terms of service to use a strongly personalised service (with consent to the merging and use of both data sets), and denying them the option to use also a less personalised version of this service (with only the On-Facebook data) would violate their basic right of informational self-determination.[83] In addition to that, the court, firstly, emphasizes "that Facebook with its social media network provides a communication platform, which at least for parts of

---

80 See Colangelo/Maggiolino (2019, 376)

81 See very clearly Robertson (2020, 177).

82 See Schneider (2018, 218-219), Costa-Cabral/Lynskey (2017).

83 See Bundesgerichtshof (2020, 47-49)

the consumers is to a large extent necessary for their participation in the social life and is of essential importance for the public discourse in political, social, cultural and political questions."[84] This leads according to the court to a special legal responsibility with regard to the conditions of the use of this platform with respect to informational self-determination.[85] The court, secondly, argues that the abusive character of this behaviour is in this case a result of both the exploitation of the consumers and the negative effects on competition, i.e. the court sees a direct link between the exploitative abuse and the exclusionary effects on the other market side, i.e. the advertising markets.[86]

The decision of the German Federal Court of Justice is a huge step in the direction of taking into account privacy concerns in competition law.[87] Although its reasoning refers solely to German law, it can be applied in a similar way also in European competition law by using the fundamental value of privacy and informational self-determination at the EU level for arguing, why the lack of choice through such a "bundling of consent" behaviour can be an abusive behaviour also according to Art. 102 TFEU. At least as important is what exactly has been decided in substance through this decision: The crucial result of this decision is that individual persons have a constitutionally protected right on a minimum standard of choice about the extent of the collection and use of their personal data, which a dominant firm is not allowed to deny them. In that context the court emphasized that the social media platform has the quality of a quasi-essential communication infrastructure in the digital society, that (for parts of the consumers) cannot be avoided anymore. This echoes the characterization of a “must-have” service in the recent CMA report. Thus, it is a particular interesting question whether this emphasis of the court should be interpreted as an additional qualification beyond market dominance in the traditional sense: On the one hand, this might imply that this approach of using this constitutionally protected right might only be relevant in exceptional cases (that go beyond mere dominance). On the other hand, this reasoning also opens up the perspective that dominant firms with this kind of essential infrastructure-like services might have to fulfill much more far-reaching responsibilities, which, e.g., might also justify a direct ex-ante regulatory approach beyond the traditional competition law.

From this perspective, it is most interesting to also look at the new proposal of a "Digital Market Act" by the EU Commission with its basic approach of introducing an ex-ante regulation (with a set of per-se rules-like obligations) for those providers of "core platform services" which qualify as "gatekeepers". One of these obligations
focusses directly on the type of abusive behaviour in the Facebook case of the FCO:

> "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." (Art. 5(a) Draft DMA).

---

[84] See Bundesgerichtshof (2020, 49: translation by the authors)

[85] See Bundesgerichtshof (2020, 41).

[86] See Bundesgerichtshof (2020, 27).

[87] See for legal analyses of this decision of the Bundesgerichtshof, e.g., Podszun (2020), Stojanovic (2020), and Witt (2020).

Here only a few comments can be made: (1) This obligation mirrors to a large extent the remedies of the Facebook case about the protection of choice of end users regarding the combination of collected personal data from different sources. (2) However such a behaviour is directly prohibited for all gatekeepers, and it is also not the result of an ex-post assessment with a balancing of interests. (3) In recital 36 of the Draft DMA it is emphasized that this obligation should support the contestability of core platform services, which would suggest a competition rationale. (4) It remains unclear whether and to what extent this obligation also takes into account privacy concerns and/or can be interpreted as a result of fairness considerations between the gatekeeper and its end users. Overall, the EU Commission acknowledges with such an ex-ante obligation the severity of the problem the FCO has raised, and supports the idea of a minimum of choice options for consumers regarding the processing and use of their personal data. However, from this proposal about regulating gatekeepers no direct conclusions follow whether the EU Commission would now view this behaviour also as an abusive behaviour according to Art. 102 TFEU.[88]

Important is that these German decisions in the Facebook case and also the DMA proposal have put a new remedy in the middle of the competition policy discussion, namely obliging firms with market (or gatekeeper) power to grant consumers a minimum standard of choice (and therefore control) over the use of their personal data. In January 2021 Germany enacted a far-reaching amendment of German competition law, which includes a similar provision about a minimum of choice regarding the provision of data both for end and business users with respect to the behaviour of firms with a "paramount significance for competition across markets" (§ 19 (2) No.4 GWB), which is the equivalent to the gatekeepers in the DMA proposal.[89] All of this is is a far-reaching development in competition policy. It is however an open question, how high the appropriate minimum standard of choice should be, i.e. what extent of granularity of choice the consumers should have.[90] It is also not clear, from which normative criterion such a minimum standard of choice is ultimately derived: Is it derived from privacy protection and informational self-determination (as in the FCO or Federal Court of Justice decisions) or from contestability and fairness (as in the DMA proposal), from the objective of consumer empowerment (consumer policy), or from an autonomy-based

---

88 It is therefore also not clear whether and to what extent the EU Commission changes its very reluctant approach of taking into account privacy effects in traditional competition law, like, e.g. in merger reviews. See for the very controversial discussion about the recent Google/Fitbit merger the deep concerns in Bourreau et al (2020), the decision about the clearance of the merger subject to conditions (European Commission 2020b), and for a critique of this decision, e.g. BEUC (2020).

89 Although this provision in Germany is not an ex-ante prohibition, it is also broader than Art.5 (a) Draft DMA, because it is neither limited to personal data nor to end users but grants a minimum of choice also to businesses with regard to their data provision vis-a-vis these powerful digital firms.

90 A very interesting solution would be that, for example, gatekeepers would have to offer consumers always a choice between a core platform service with and without having to provide personal data (e.g. by having to offer the service also with a monthly subscription fee and without the collection of data). See for such a policy proposals Becker (2017).

concept of freedom of choice (or a combination of them)?[91] These are important and urgent questions that need much further discussion.

5.5 The importance of remedies or why competition law might not be enough

In our theoretical chapter 3 about the implications of the simultaneous existence of two market failures and two policies we have only briefly mentioned the role of remedies but did not analyze them in detail. However remedies play a key role not only for the effectiveness of both policies but also for their relationship, especially if negative effects on competition and privacy might be jointly caused by both market failures. In this section we will briefly discuss the potential effectiveness of the remedy of the FCO in the Facebook case. The FCO has chosen a new innovative form of an "unbundling remedy", namely the requirement of an additional consent of the consumers to the merging of the personal data collected within and outside of the Facebook services. Consumers should have the option to use the social media platform of Facebook also without having to give their consent to the integration of all these personal data. Without this consent Facebook has to keep these two sets of data separate (internal unbundling).[92] But can we expect that this remedy of the FCO is effective with respect to the alleged exclusionary and exploitative effects?

Regarding the exclusionary effects on competition it is very unclear, whether a sufficiently large enough number of users of the Facebook social media platform will use this additional option in that way that they do not give consent to the integration of their data. If many users would still give their consent (e.g., because Facebook incentivizes this consent or uses other behavioral targeting instruments for nudging users to give their consent), then this remedy can be expected to be too weak for reducing the exclusionary effects in a sufficient way.[93] From a competition perspective a direct prohibition of the bundling of both sets of personal data, independent from the consent of the users, would be a much more consequent remedy for solving the problem of superior data advantages of Facebook regarding competition on other markets.[94] Such remedies are, e.g., sometimes used in data merger cases, where keeping certain sets of data of the merging firms separated can be a condition for clearing the merger.[95] This also shows that requiring an additional consent for integrating these data is much more a data protection remedy than a competition remedy.

---

[91] See Podszun (2019; 2020, 1273-1275).

[92] See Bundeskartellamt (2019c, 1-2). Such a remedy can also lead to complex problems, because then Facebook might have to offer several versions of its service, with and without such a data integration, and perhaps also with a monetary price (for a version without data integration) and the ensuing question what price might be seen as still acceptable (see Colangelo/Maggiolino, 2019, 372).

[93] This can also be described as a "collective action" problem of the users. Only if many users do not agree to the merging their data, a positive effect on competition can emerge.

[94] See, e.g., Condorelli/Padilla (2020, 184), who discuss this option as a privacy regulation remedy against envelopment strategies through "tying of privacy policies". However any limits for integrating data sets can also lead to efficiency losses through less data aggregation.

[95] See, e.g. OECD (2020, para.148).

At first sight it looks easier with regard to the exploitative effects of the "bundling of consent" behavior on privacy. Here the requirement of an additional consent for combining the two data sets directly increases the choice options of the users, and therefore gives them more control over their personal data. Through denying their consent to the integration of both data sets, they can reduce (to some extent) the additional privacy risks from combining their personal data, and can choose better according to their own privacy preferences whether they want to use a more or less personalised version of the services of Facebook. If we use - as discussed in the last section 5.4 - the criterion that users of such services like the Facebook social media platform should have a minimum of choice options with respect to the collection and use of their personal data, then this remedy can directly help. It is, however, still an open question whether this remedy offers sufficient choice options, e.g., for protecting the constitutionally protected right of privacy and informational self-determination. However the main problem of this remedy of granting a choice is that we still have the additional information and behavioral market failure problem, which is not solved by this remedy. If many users of the Facebook services do not understand the impact of this additional consent, also due to intransparency and unawareness of the large amount of collected data through third-party websites, online-tracking, and other sources, then they can be in a similar way overwhelmed by this additional option as they are in many other situations where they face "notice and consent" solutions. Then it is very unclear whether this additional option for choice can really be effective in solving their problems of protecting their privacy and making rational, well-informed decisions about the provision of their data with respect to the ensuing privacy risks and their privacy preferences.[96]

Our brief discussion of the remedy of the FCO in the Facebook case makes clear that despite some positive effects through providing more choice options to the consumers, its effectiveness regarding both competition and privacy might be rather limited and presumably insufficient. Please note that the new proposed obligation for gatekeeper platforms in Art. 5 (a) of the Digital Market Act runs into exactly the same problems. One important reason is that the remedy of an additional choice does not solve the the second market failure of information and behavioral problems. It can be discussed whether a competition authority might also be capable of applying more effective remedies that help to solve information and transparency problems of consumers, e.g. by prohibiting "concealed data practices"[97] or requiring minimum standards for transparency about data collection and privacy terms. However the remedies of competition authorities for solving information and behavioral problems of consumers will always remain limited.

As a consequence, it might have to be accepted that in such cases with two market failures the application of competition law alone might not be sufficient for solving the problems, and it might be necessary that also data protection and/or consumer law have to get active for contributing with their remedies to the solution of the problems. If, in particular, we take into account the interaction effects between the two market failures, which imply that the negative effects on competition and privacy are jointly

---

[96] To some extent the FCO has taken this problem into account in its remedy by requiring that Facebook present solutions with regard to its terms of service and its data collection practices, which will increase transparency (Bundeskartellamt 2019b, 1-2). It is however not clear whether this is sufficient for solving the second market failure.

[97] See, e.g., Kemp (2020).

caused by both market failures, then it would not be surprising from an economic perspective that these problems might need a sophisticated combination of remedies of competition law and data protection / consumer law. In our final chapter 6 we will discuss the implications for the relationship between competition law and data protection law.

6. The need for a broader and more integrated policy approach

What are the most important results of our analysis? Since we have a problem of the simultaneous existence of two market failures with considerable interaction effects between them and between these policies on digital markets, the main counter argument against the Facebook case that privacy concerns should not be taken into account in competition law but only in data protection law, is untenable and cannot be defended any more. Since data protection law is not capable of dealing with the negative effects of competition problems on privacy, the application of competition law in such cases as the Facebook case is appropriate and often necessary. The main approach of the FCO in its Facebook decision to challenge this "bundling of consent" requirement in the privacy terms as an abusive behaviour of a dominant firm, because it restricts too much the choice options of users, is convincing and can be supported. It was confirmed by the German Federal Court of Justice, and is now even included in the set of general obligations for gatekeeper platforms in the DMA proposal at the EU level. Therefore the Facebook case is a very important precedent case both for taking privacy concerns into account in competition law and for protecting a minimum level of choice options against the market power of large digital platform firms. Instead of deriving directly the abusive character from a violation of data protection law, it is more appropriate to take into account the effects of such a behaviour on competition and privacy in a broader approach of balancing of interests. However, much more research is necessary, with regard to both the relevant normative criteria and the effects of data-collecting behaviour of dominant firms on privacy and on competition.

It is also an important result that competition law alone cannot solve the problems in a sufficient way. Although a decision like in the Facebook case of the FCO can contribute to mitigate the negative effects, it can do this only in a limited, and presumably not sufficiently effective way. Particularly with regard to the problem of the collection and use of personal data of large digital platform firms, in which both serious privacy problems as well as huge competition problems emerge, it might be necessary that both policies are actively trying to solve the problems, and in this respect also collaborate with each other. Although in several countries competition authorities and data protection authorities have already started to have contact with each other, and are using in some cases already the advice of the other authority in their own proceedings, both types of authorities are still far away from an effective collaboration. In the following, some policy options for a more collaborative and integrated approach of competition law and data protection law are discussed.[98]

Collaboration between competition and data protection authorities can be possible in different ways. For example, these controversial "bundling of consent" terms of service of Facebook could be the subject of parallel or joint investigations of both competition

98 See for some recent contributions to this discussion, e.g., OECD (2020, 50-52), Graef/van Berlo (2020), and, in a more general and broader way, Reyna (2021).

and data protection authorities. A close collaboration of the authorities might lead, first, to a much better analysis and understanding of the problems, also through exchange of information and mutual discussion from the different perspectives of competition and data protection law, and, might allow, secondly, also a better assessment, what role each of these policies could play in such a case, and what combination of remedies might be most effective for solving these problems. Competition and data protection authorities can also jointly develop guidelines about data-collection behaviour and privacy terms that would consider both privacy and competition concerns, and also deal with potential trade off-problems between competition and privacy protection, e.g. with respect to data-sharing remedies. These guidelines could also entail minimum standards for choice options for consumers or principles of internal unbundling of data sets within conglomerate digital platform firms with dominant market (or gatekeeper) positions.

Beyond a collaboration of competition and data protection authorities with respect to the application of both laws, it is also necessary to ask how competition law and data protection law can be improved for solving better the common problems and avoid conflicts with respect to their objectives. This requires a deep analysis of the interaction effects between both types of market failures and both policies (see chapter 3). Particularly important are trade off problems between competition and privacy protection, because the strict privacy protection of the GDPR can have negative effects on competition (through de facto strengthening large digital platform firms). Here the enabling of a larger differentiation of the data protection rules for firms with market power (or larger firms) with regard to data collection and privacy terms in comparison to other firms might be an important reform option that can help to mitigate competition problems. Vice versa, a more effective competition policy, e.g. through a more privacy-enhancing application of competition law or the introduction of an effective ex-ante platform regulation, can also help to protect better the privacy of consumers. Another wellknown discussion refers to making the data portability right of Art. 20 GDPR more effective for helping to solve competition problems. All these discussions show the complexity of the relationship between competition law and data protection law, and the need to improve and better align both policies. This also refers to their tool-box of remedies and the institutional set-up for such a more integrated and collaborative approach.

However the relationship between competition law and data protection law has also to be seen in the wider context of the entire legal and regulatory framework for the digital economy. In addition to the already mentioned consumer policy, also the emerging new field of data (governance) policy, intellectual property rights, and interoperability / standardisation policy are particularly relevant, because they also can have far-reaching effects on the policy objectives competition, innovation, privacy, and consumer protection. This also includes the need for taking into account additional market failures, e.g. with respect to innovation, interoperability and standardisation, and data-sharing and data aggregation. From an economic perspective, it can be expected that between all of these policies significant interaction effects exist, leading to the need for a much more comprehensive and deep analysis of the interplay between (all of) these policies. This insight into the relevance of this interplay between different market failures and

policies strongly supports the demand for a more holistic and integrated policy approach in the digital economy.[99]

Also additional specific regulations as the Digital Market Act, the Digital Services Act or sector-specific regulations can be important building-blocks within such an integrated policy approach. How does the current proposal of the Digital Market Act fit into such a perspective? On the one hand, we have already seen in section 5.4 that the alleged abusive behaviour in the Facebook case has found its way into the list of behaviours that are per-se prohibited for gatekeepers, and that therefore the EU Commission supports the main idea of the German FCO (and the Federal Court of Justice) that consumers should be granted a minimum standard of choice about the use of their personal data vis-a-vis powerful platform firms. On the other hand, the DMA does not address its relationship with data protection law (except that the GDPR has to be fully respected). It is unclear whether the obligation of Art.5(a) Draft DMA also should mitigate privacy concerns through gatekeepers or is justified only by competition and/or fairness concerns. The DMA also does not entail any provisions for a closer collaboration with data protection authorities, e.g., with respect to privacy protection issues in the context of data-related obligations (data access, data portability). Therefore the DMA proposal so far does not seem to contribute much to a closer and more collaborative relationship between competition policy and data protection law (despite the key role of personal data for gatekeepers). However the DMA also does not address the relationships (and collaboration) with other policies, as, e.g., consumer policy with its objective of more consumer empowerment, although some obligations, which strengthen the choice of end users, could also be interpreted as consumer policy.[100] Therefore they might fit into the manifold discussions in consumer policy about strengthening consumer empowerment by giving consumers more control over their data. But the DMA does not clarify, whether it also wants to contribute to the objectives of consumer policy.

Therefore it is unclear to what extent the DMA proposal is embedded into a more collaborative and integrated policy concept about protecting competition and privacy, fostering innovation, and empowering consumers. This seems to be different in the recent proposal of the CMA of a new ex-ante regulatory regime for the powerful digital firms with Strategic Market Status in the UK. The CMA proposal is embedded in a much clearer framework regarding market failures and other policies, especially consumer and data protection policy, and emphasizes the importance of collaboration of the proposed "Digital Market Unit" with the enforcement agencies of the other policies.[101] Therefore it can be recommended that the proposal of the Digital Market Act could be improved by clarifying more the relationships to data protection and consumer law and by including provisions for enabling and encouraging a closer collaboration with other policies, in particular, data protection law.

---

99 See, e.g., EDPS (2014), Kerber (2016, 647), Graef/van Berlo (2020), as well as Kerber (2019, 40) for using also the interplay with other policies for dealing with the competition problems through large online platform firms.

100 In the DMA proposal the obligations in Art. 5(a), 5(c), 5(f), 6(1)b, 6(1)c, 6(1)d, 6(1)e, and 6(1)h strengthen the rights of consumers and can therefore also be seen as consumer policy.

101 See CMA (2020b, 75-78).

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, 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.

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.

Averitt, N.W./Lande, R.H. (2007). Using the "Consumer Choice" Approach to Antitrust Law, Antitrust Law Journal, 74, 175-264.

Ayata, Z. (2020). Old abuses in new markets? Dealing with excessive pricing by a two-sided platform, Journal of Antitrust Enforcement, jnaa008, https://doi.org/10.1093/jaenfo/jnaa008

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

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

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

Bishop, S./Walker, M. (2010). The Economics of EC Competition Law: Concepts, Application and Measurement, Sweet & Maxwell, London, UK.

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

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.

Bundesgerichtshof (2020). Order of 23.06.2020, Case KVR 69/19.

Bundeskartellamt (2019a). Decision no B6-22/16 of 6 February 2019. An English translation is available at: www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

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

Bundeskartellamt (2019c). Press release - Bundeskartellamt prohibits Facebook from combining user data from different sources, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2

Budzinski, O./Grusevaja, M./Noskova, V. (2020). The Economics of the German Investigation of Facebook's Data Collection, Ilmenau Economics Discussion Papers, 26 (139), https://www.tu-ilmenau.de/fileadmin/public/wth/Diskussionspapier_Nr_139.pdf

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

Buttarelli, G. (2019). This is not an Article on Data Protection and Competition Law, CPI Antitrust Chronicle February 2019.

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

CMA (2020a). Online platforms and digital advertising – Market study final report, July 2020.

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

Colangelo, G./Maggiolino, M. (2018). Data Accumulation and the Privacy–Antitrust Interface: Insights from the Facebook case, International Data Privacy Law, 8(3), 224–239.

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

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, Jacques/de Montjoye, Yves-Alexandre/Schweitzer, Heike (2019). Competition Policy for the digital era – Final report.

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

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

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

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

Esayas, S. (2017). Privacy-as-a-Quality Parameter: Some Reflections on the Scepticism, Stockholm Faculty of Law Research Paper Series, 43, Stockholm University, Sweden.

Esayas, S. (2018). Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law, International Data Privacy Law, 8(3), 181-199.

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

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

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

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

Furman, J./Coyle, D./Fletcher, A./McAuley, D./Marsden, P. (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.

Graef, I./Clifford, D./Valcke, P. (2018). Fairness and enforcement: Brdging 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

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

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.

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. (2009). Should competition law promote efficiency? Some reflections of an economist on the normative foundations of competition law, in: Drexl, J./Idot, L./Moneger, J. (eds.), Economic theory and Competition Law, 93–120, Edward Elgar, Cheltenham, UK.

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. (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

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

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

Krämer, J./Senellart, P./de Streel, A. (2020). Making data portability more effective for the digital economy – Economic implications and regulatory challenges, Centre on Regulation in Europe (CERRE).

Lancieri, F. (2021). Narrowing Data Protection's Enforcement Gap, mimeo.

Lipsey, R.G./Lancaster, K. (1956). The General Theory of Second Best, Review of Economic Studies, 24 (1), 11–32.

Lynskey, O. (2018). Non-price Effects of Mergers - Note (OECD DAF/COMP/WD(2018)70 (6 June 2018)

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

Manne, G.A./Sperry, R.B. (2015). The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework, CPI Antitrust Chronicle, May 2015 (2).

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

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

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

Podszun, R. (2019). Digital ecosystems, decision-making, competition and consumers – On the value of autonomy for competition, https://ssrn.com/abstract=3420692

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

Reyna, A. (2021). Breaking Down Silos in Public Enforcement. Lessons from Consumer-Facing Markets, mimeo.

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.

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.

Schweitzer, H./Haucap, J./Kerber, W./Welker, R. (2018). Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Nomos, Baden-Baden, Germany. Also available at: https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.html.

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.

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.

Stigler Committee on Digital Platforms (2019). Final Report, https://www.chicago-booth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf

Stojanovic, M. (2020): Can competition law protect consumers in cases of a dominant company breach of data protection rules? European Competition Journal 16/2-3, 531-569

Stucke, M.E. (2018). Should we be concerned about Data-Opolies?, Georgetown Law Technology Review, 2, 275–324.

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.

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

Waldman, A.E. (2020). Cognitive Biases, Dark Patterns, and the 'Privacy Paradox', Current Opinion in Psychology 31, 105-109.

Witt, A.C. (2020). Exploitative Abuses in The Age of Dominant Digital Platforms – The German Facebook Case, forthcoming in: The Antitrust Bulletin, 66(2).