DATA PROTECTION AND ANTITRUST: NEW TYPES OF ABUSE CASES? AN ECONOMIST'S VIEW IN LIGHT OF THE GERMAN *FACEBOOK* DECISION

BY JUSTUS HAUCAP[1]

1 Professor of Economics at the University of Düsseldorf, Director of Düsseldorf Institute for Competition Economics ("DICE"). Disclaimer: Two years ago, the author wrote a short expertise on the role of data in social networks on behalf of Facebook. He has neither been active for Facebook since then nor has he discussed any details of the German *Facebook* case with either Facebook or any of its representatives since then. The author is also a member of the German Federal Cartel Office's economics expert working group on competition economics.

I. INTRODUCTION

Many services on the Internet are seemingly offered for free, people do not have to pay for them, at least not with money. Instead, it is regularly argued, people are paying with their (personal) data. If people are not paying with money, but with data, however, the question emerges how antitrust laws can be applied to these particular markets.

How difficult it is to define markets in the absence of monetary prices has been discussed in the literature at length by now. Less attention has been given to the question of whether and, if so, how data protection and privacy concerns should be part of antitrust enforcement. Three different issues can be distinguished in this context. First, there is the question of what kinds of behavior (if any) may be considered exploitative abuses by dominant firms in markets where customers are not paying with money, but – as it may seem – with data. This is, by and large, at the heart of the Federal Cartel Office's *Facebook* case in Germany, the decision of which has long been eagerly awaited and was finally announced on February 7, 2019, even though the text of the decision has not been published yet.[2] Second, a question emerges whether denying competitors access to certain types of data may be considered an obstructive abuse or anticompetitive exclusionary behavior that unduly impedes effective competition. And third, a question arises whether the effects that arise from the acquisition and combination of data sets should be subject to distinct consideration in merger analysis.

II. DATA USAGE BY DOMINANT FIRMS AS EXPLOITATIVE ABUSE?

Let us start with analyzing the first question, which is also decisive for the German *Facebook* case: What kind of behavior constitutes an exploitative abuse in markets where people do not pay with money for the services they use? In principle, the underlying idea pursued by the Federal Cartel Office appears to be quite simple: Excessive pricing by dominant firms is unlawful in many countries, for example under Article 102 of the Treaty of the Functioning of the European Union. Hence, once users are "paying with data," a dominant Internet firm's use of customer data may also be considered excessive. Put differently, if a firm asks its customers for "too much" data and is "too intrusive" with respect to users' privacy in return for its services, this may be considered an exploitative abuse of market power analogous to excessive pricing. However, as is often the case with simple ideas, things become more complicated at second sight.

First of all, data is not like money. Providing personal data to an online service does not reduce the user's ability to provide the same data to another service or multiple other services. Hence, while in public discussions data is often portrayed as "the new oil" or as a means of payment,

2 The Federal Cartel Office published a summary of the case on February 15, 2019, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf.

these analogies are highly misleading. Oil is an exhaustible resource and a private good that cannot be used either in parallel or sequentially by different users, while data can be used multiple times and at the same time by many services. Similarly, the idea that data is a means of payment is misleading, as – unlike money – the same data can be shared with multiple users multiple times. Even if a user "pays" with data for a particular service, the user's amount of data available to him or her is not reduced. His or her wealth in terms of available data is not affected. In that way, "paying with data" is quite unlike paying a monetary "price." Hence, it is conceptually much more difficult to construct an exploitative abuse case, as users are not left with less data than they had before. This is a fundamental difference to excessive pricing cases where customers are left with less money/wealth once they have been exploited. If a resource can be used infinitely often without incurring any additional cost, however, it is not possible to exploit that resource or its holder.

However, while users may not be exploited with respect to their data, their privacy may be reduced, possibly unduly so. In fact, this view is closer to the FCO's theory of harm. According to the FCO, Facebook's behavior is exploitative *vis-à-vis* its users because users are losing control about how their data is used.[3] Still, for a reduction in personal privacy (and excessive data requirements) to be similar to a reduction in personal wealth (and excessive pricing), people actually need to care about privacy. At this point, it is noteworthy that, quite generally, many people willingly consent to other parties' using their personal data if this increases the quality of the services they are interested in. While it is true that many people, when asked in public, maintain that they are concerned about how their personal data is used and that they are rather protective about how their data is used, these stated preferences are not revealed in their actual behavior. Put differently, a substantial body of empirical and experimental evidence has consistently found over and over again that even a vast majority of individuals who maintain to be heavily concerned about privacy are willing to share personal data in return for rather small forms of compensation or improved services.[4] This finding has been coined the "privacy paradox."[5]As, however, preferences revealed through actual behavior are typically taken to better reflect individuals' true preferences than surveys, it appears that many people willingly share their data in order to obtain better services. Given these findings, it is difficult to conceive how users can be exploited if they willingly share their data. Overall, however, we may need to broadly distinguish between two types of potential users: Those who really care about their personal data and their privacy and those who do not, but happily share their data.

If users of a particular Internet service do *not* mind if their personal data is used by the service provider, this means that they do not receive disutility from sharing personal data and having data sets combined. In these cases, collecting and combining data from these users can hardly be an exploitative abuse, as consumers cannot be exploited if they do not mind providing the data that is collected. Put differently, there can hardly be any harm inflicted onto these users if they do not receive any disutility from having their data combined. On the contrary, as combining data typically facilitates the development of better matching technologies to rank offerings, news, and other information to match user interests, the prohibition to do so would lead to a deterioration of the services offered (as the matching technology would deteriorate).

In addition, as a rule of thumb, it appears safe to assume that users at least weakly prefer advertising that matches their interests over advertising that does not coincide with their interests ("spam" at the extreme). Hence, better matching users and advertisers should, if at all, increase users' utility from using a particular service and clearly increase the benefits that accrue to both users and advertisers. Put differently, the quality of a platform's matching technology does not only affect advertisers, but also tends to benefit users. Generally speaking, the quality of any matching technology depends, in part, on the amount, but also on the quality of information available to be used by the technology, along with a host of other factors. Hence, the benefit received from a particular service, for both users and advertisers, is a positive function of the amount and quality of information available to be used to match users with content that may interest them, both organic and advertising. In this context, access to and use of different sources of data (e.g. off-Facebook data and on-Facebook data, which is at the heart of the German *Facebook* case) allows for better matching than the use of just one source.

The case is different, of course, once we assume that (a) either a sufficient number of consumers do actually receive disutility from "excessive" data requirements and from having their data combined or (b) consumers are somehow being harmed without noticing it. But even for these cases, it is not clear that antitrust laws are best for dealing with these valid concerns. Virtually all jurisdictions have specific laws regarding data protection and privacy that typically apply to all firms and transactions regardless of market power. It is obvious that firms with market power have to adhere to these standards in the same way as firms without (substantial) market power. It is unclear though, at least from an economic

3 See Bundeskartellamt (2019), Facebook FAQ's, online at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf.

4 See, e.g. Acquisti, A., C. R. Taylor & L. Wagman (2016), "The Economics of Privacy," *Journal of Economic Literature* 54, pp. 442-492; or Benndorf, V. & H.-T. Normann (2018), "The Willingness to Sell Personal Data," *Scandinavian Journal of Economics* 120, pp. 1260-1278.

5 See Norberg P. A., D. R. Horne & D. A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41, pp. 100-126.

perspective, why a breach of privacy and data protection laws would also, in addition, constitute a breach of antitrust laws. Put differently, since a breach of data and privacy laws by firms without market power cannot be an antitrust abuse, why would the same behavior by dominant firms constitute a breach of antitrust laws? The question appears to be whether antitrust laws should hold dominant firms to stricter data protection and privacy standards than competing firms without market power are held to by general data protection and privacy laws. From a competition policy perspective, it is difficult to conceive of good reasons for such a policy.

In fact, hypothetically requiring dominant firms to use or combine less data or only data from certain sources and to offer higher privacy standards than what is legally required from competing firms without market power would be equivalent to requiring dominant firms by law to offer – from the perspective of those users who heavily care about privacy - superior products than rivals – a requirement, which could – in the extreme case – even foreclose the market, as data-sensitive consumers would basically be guaranteed higher privacy standards with dominant firms.

At the same time, a dominant firm in the "user market" may become less competitive in advertising markets *vis-à-vis* competitors form other "user markets." And, finally, as data is used to develop and offer better services at least in the eyes of those consumers who do not mind sharing their data, preventing firms from collecting, combining, and using data beyond what is regulated by privacy and data protection laws is equivalent to requiring the firm to be less innovative and to offer inferior services – both of which would harm competition.

Still, a situation may emerge where dominant firms can "force" their users to consent to the use and combination of levels of data which non-dominant firms may not be able to obtain from their customers. In fact, this appears to be the FCO's key objection regarding Facebook. The dominant firm's access to more data is likely to help the firm to improve and tailor its services to user preferences and also to increase advertising efficiency. Here a difficult trade-off emerges, as requiring dominant firms to collect and to combine less data will typically also imply a deterioration of service quality and advertising efficiency, and thereby, a softening of competition. While some consumers may prefer higher privacy standards even if this reduces service quality, other consumers may happily share their data in exchange for better-tailored services. In the past, therefore, the idea has been brought forward that dominant firms should be forced to offer consumers two forms of "payment": Consumers should be free to either pay with their data or with their money. There are several problems with this suggestion, however. First, it is unclear what the competitive price in monetary terms should be, given that it has not emerged in the market for most services that are under consideration. Second, firms use the information not only to improve advertising efficiency, but also the product itself. Hence, the more consumers chose to pay with money, the lower the service's quality will inherently become, as data is a critical input to improve the services. While users who do not provide data may individually receive lower service quality levels, the overall quality of a matching algorithm will also deteriorate as less information on users' preferences and behavior is available.

Consider the case of social networks as an example: Typically, social network users are fairly heterogeneous in their motives as to why they use social networks. While some users tend to be more active and send out and share personal information, comment on other users' activities, and engage in discussions, other users tend to be more passive and, instead, receive and consume information provided by other users (i.e. they may "follow" others' activities rather than using social networks as a "broadcasting" medium). Of course, many people tend to engage in both information sharing and consuming activities at various times, but for analytical purposes it is helpful to distinguish between sharing and consuming activities, keeping in mind that users are "senders" at one point in time and "receivers" at others. "Senders" tend to benefit if they are able to reach interested "receivers," while "receivers" benefit from relevant information broadcasted by "senders," as this increases the likelihood of receiving interesting or engaging content.

It is important, though, to note that the user benefits of sending and receiving information do not simply increase with the amount of information received and the number of potential receivers addressed. If "senders" share information with many people, but most "receivers" do not find the information useful or interesting, the "sender" may not really benefit from sending out the information- just as commercial advertisers do not benefit if they target the wrong audience. Similarly, "receivers" do not benefit from an increase in the amount of information if they find the information offered uninteresting and useless. Quite in contrast, receiving more information of little interest (which may be considered "spam") will even decrease "receivers'" utility, as they will find it more difficult to sort out the more interesting updates from the less interesting ones, especially if such an increase in information leads to information overload. Hence, both "senders" and "receivers" tend to benefit from better matching technology. "Receivers" benefit the better the information highlighted to them is. Similarly, when users share information they benefit if the information they share primarily reaches people who are interested in that particular information. If, in contrast, the information shared is received by users who do not find that information useful or neglect it, the "sender" receives less benefit from sharing his information, assuming that people share information with the purpose of reaching an audience who finds the information useful or interesting. If the matching mecha-

nism for information shared and information received is improved, user benefits increase. Hence, better matching any type of content with user interests increases the utility of the social network for both "senders" and "receivers."

Finally, forthcoming empirical evidence even suggests that larger firms often tend to offer more privacy than small ones.[6] Hence, it becomes unclear which privacy level would prevail at the competitive level – the standard hypothetical counterfactual for antitrust abuse cases – and which level would be considered abusive.

In its *Facebook* case, the German competition authority is particularly concerned about Facebook's practice of collecting data from outside the Facebook universe. In fact, Facebook collects data about its users and even non-users via apps such as WhatsApp and Instagram that are owned by Facebook and also via third-party apps and webpages that use Facebook interfaces, for example, in the form of Facebook-like-buttons that are integrated in many webpages. However, while these practices may possibly violate privacy and data protection laws, it is still unclear how they relate to Facebook's market power, and whether and how consumers are exploited beyond the harm possibly inflicted by potentially violating privacy and data protection laws.

In sum, Internet users and advertisers both tend to benefit from the use and combination of data, as the usage and combination of different data sources facilitates the improvement of matching algorithms to offer services, rank information, and provide news for users. The case is different, however, if some users receive direct disutility from their data being used. In these cases, however, data protection and privacy laws appear to be the proper statutes to regulate firms' behavior. It is not clear from an economic perspective why firms with market power should be held to stricter privacy standards than firms without market power, as such a practice may distort, rather than protect, competition. Moreover, it is at best unclear whether small firms adhere to stricter privacy standards than large firms. If, however, the opposite is true, the question emerges what the appropriate benchmark for abuse cases should be. Requiring dominant firms to behave more like competitive firms would be rather absurd if small firms without market power violate privacy standards more often than larger firms.

The FCO also suggests that users may not always be aware of what kind of data is collected and how this data is used due to a lack of transparency. This, however, appears to be by and large a problem of asymmetric information which is not necessarily related to market power. Put differently, information asymmetries are often also exploited in competitive markets with small firms, as George Akerlof already suggested in his famous used car dealer example.

Also, any analogy with data as a form of money or payment is misleading, as monetary resources cannot be used multiple times. Finally, empirical evidence suggests that (many) people do not feel exploited when their data is used. Quite in contrast, a fair number of people tends to willingly share data in order to obtain benefits such as improved services. This is probably especially true for social networks where many people "broadcast" personal information about their activities. Against this background, it is conceptually rather difficult to establish sound evidence that collecting and combining users' data constitutes an exploitative abuse of market power, especially when considering the fact that small networks and Internet service providers without market power also engage in comparable practices.

III. DATA USAGE BY DOMINANT FIRMS AND OBSTRUCTIVE ABUSE OF MARKET POWER?

At least from a conceptual point of view, situations in which dominant firms deny third-party access to certain types of data may be more easily conceived as an (obstructive) abuse of market power. Put differently, situations may emerge in which – due to network effects and economies of scale – a dominant firm has collected such an amount of data that competitors may not be able to duplicate the same or a functionally equivalent set of data and, therefore, suffer from a substantial competitive disadvantage. In the extreme case, certain data may be considered an essential facility to which competitors need access, unless there are valid justifications for not grating access- such as, for example, privacy and data protection laws. Nevertheless, depending on the particular circumstances, sometimes even anonymized or pseudonymized data may be sufficient to facilitate competition. For the Google search engine, for example, some authors have argued that granting third party-access to historical search and click data would solve most of the competition concerns.[7]

6 Sabatino, L. & G. Sapi (2019), "Online Privacy and Market Structure: An Empirical Analysis," DICE Discussion Paper No. 308, available online at https://ideas.repec.org/p/zbw/dicedp/308.html.

7 Argenton, C. & J. Prüfer (2012), "Search Engine Competition with Network Externalities," *Journal of Competition Law and Economics* 8 (1), pp. 73-105.

From an economic viewpoint, there are good reasons why, in principle, third-party data access should be granted more easily than in the case of classical essential facilities such as physical networks or other infrastructure. First, classical infrastructure is often rival in usage. Once a competitor has taken over the incumbent's local loop, the incumbent cannot use the relevant lines itself anymore. Similarly, if a certain slot for a railway track is used by a new entrant, the same slot cannot used by the incumbent any longer. In contrast, even with third-party access to data, the incumbent can still use the data itself. Hence, access to assets or facilities that are not rival in usage should be granted more easily. Second, physical infrastructure typically requires significant investment and maintenance expenditures. Therefore, antitrust law and regulation have established rather high legal thresholds for third-party access in order to preserve the investment and maintenance incentives. In contrast, while data collection and maintenance can also require significant investment, this is not always the case. Instead, data is often generated and collected as a by-product without significant investment efforts by the collector. If, then, incumbents can collect data without significant investment, the threshold for third-party access should be systematically lower than for traditional essential facilities.

Overall, the fact that (a) data is typically non-rival in usage and (b) data is at least sometimes collected by incumbents without significant investment together suggest that the threshold for third-party access should, in principle, by systematically lower than for classical infrastructures. Data protection and privacy laws play a role in these cases; however, they may also provide valid justifications for why third-party access to data may not be granted in some cases.

In the FCO's prominent *Facebook* investigation mentioned above, access to data or data sharing has not played any role. However, the FCO's second theory of harm circles around the effects that Facebook's data collection efforts have on competitors, more precisely the effects of Facebook's data collection activities in advertising markets. Interestingly enough, the FCO has found Facebook to be "the dominant supplier of advertising space in social networks," suggesting that "advertising in social networks" is a separate antitrust market in its own, separate from other online advertising markets. It remains to be seen what evidence there is to suggest that Google (which does no longer operate social networks, as YouTube does not appear to be part of the relevant market in the FCO's eyes) and Facebook do not compete for online advertising in the same market. Be it as it may, the FCO's theory of harm with respect to advertising markets mainly consists in Facebook being able to collect and combine so much data that it can easily outcompete its rivals, as it can better target advertising – by and large an efficiency offense, which may even benefit users if they prefer more targeted advertising over advertising that is less related to user preferences.

IV. DATA PROTECTION AND MERGER POLICY

Finally, new challenges emerge for merger policy, as the potential combination of data sets may give rise to new competition concerns not only in horizontal and vertical, but also in conglomerate mergers. In many instances, however, the combination of data sets will give rise to new efficiencies as long as the combination of data sets either increases the productivity of production and/or distribution activities, or facilitates the supply of tailor-made products or services. Moreover, data protection and privacy laws obviously also apply to merged entities. As long as data protection and privacy laws regulate firms' behavior with respect to their usage of data, there does not appear to be an additional role for merger policy with respect to data protection.

In the context of the FCO's *Facebook* case, an interesting observation is that the FCO has chosen a rather narrow market definition for social networks, explicitly excluding WhatsApp from that market. While this is certainly helpful for the FCO in bringing its abusing case, it also contrasts with thinking by the European Commission's chief competition economist Tommaso Valletti whether we should not define markets for attention (which is truly a scarce resource). From a merger policy perspective, defining markets for attention is, of course, attractive for competition authorities as it allows them to tackle Facebook's acquisitions of WhatsApp and Instagram more easily. Abuse cases, however, become more difficult under such a market definition, as it would be much less clear whether Facebook would be dominant in a market for attention. In order to apply competition law in a consistent fashion, markets need to be defined in a consistent way, either as markets for attention or more narrowly, independent from whether mergers or potentially abusive behavior is investigated.

V. CONCLUSION

For many Internet services, users do not pay with money, but rather pay with their (limited) attention. While users are sometimes said to pay with their data for these services, this analogy is rather misleading, as users' data is, unlike money, not limited – quite in contrast to users' attention. As data is, in principle, not limited, it is much more difficult to conceive what use of data would constitute an exploitative abuse of market power – the issue which is at heart of the German antitrust case into Facebook's data combination practices. Moreover, since data is typically used to improve the respective services, it should be much more difficult to provide sufficient evidence that the usage of data constitutes an exploitative abuse of market power that harms consumers. In addition, as smaller networks and service providers without market power do not appear to systematically adhere to stricter privacy and data protection standards, it becomes difficult to envisage what the appropriate counterfactual should be that dominant firms need to adhere to. A hypothetical requirement for dominant firms to adhere to stricter privacy standards would, also, very likely distort rather than safeguard competition. As a consequence, portraying data usage as analogous to excessive pricing is fraught with difficulties.

In contrast, it is easier to conceive that not granting third-party access to data may be an obstructive abuse of market power. Moreover, as data is – in contrast to many other facilities – non-rival in use and, at least in some cases, not associated with significant investment expenditure, the legal threshold for third-party access should generally be lower than for classical essential facilities, such as physical network infrastructures.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.