THE GERMAN *FACEBOOK* CASE – TOWARDS AN INCREASING SYMBIOSIS BETWEEN COMPETITION AND DATA PROTECTION LAWS?

BY DR. JÖRG HLADJK, PHILIPP WERNER & LUCIA STOICAN[1]

1 Dr. Jörg Hladjk, Partner, Jones Day, Cybersecurity, Privacy & Data Protection Practice, Brussels. Philipp Werner, Partner, Jones Day, Antitrust & Competition Practice, Brussels. Lucia Stoican, Associate, Jones Day, Antitrust & Competition Practice, Brussels. The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.

CPI ANTITRUST CHRONICLE FEBRUARY 2019

I. INTRODUCTION

The rise of multi-sided online platforms like Amazon and Facebook, that collect, process, and monetize huge amounts of users' data for profiling and targeted advertising has created controversial issues under both competition and data protection laws. This has especially been accentuated in Europe due to the entry into force of the GDPR in May 2018[2] and due to the recent spotlight on tech companies – coming from both competition and data protection enforcers.[3]

Competition authorities around Europe have expressed concerns that – while data becomes "the oil of the 21st century" – a handful of companies are gaining control over it and "real competition" for the market becomes virtually impossible. The identity crisis of the rule of law system in the tech area is evident in a recent statement of EU Commissioner Margarethe Vestager: "we do not know if we should just reinterpret the rules we have already or to what degree we should add new rules."[4]

The struggles of an obsolete rule of law system to deal with high tech and big data are also reflected in recent decisions. While in the *Facebook/Whatsapp* merger, the European Commission summarily noted that "privacy-related concerns flowing from the increased concentration of data within the control of one company (…) do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules,"[5] in the subsequent *Microsoft/Linkedin* case the Commission nuanced its position and clarified that "privacy-related concerns (…) can be taken into account in a competition assessment to the extent that con-

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

3 Europe, in particular, has focused significant attention on competition, big data, and regulation of digital platforms. Recent landmark cases in the EU include the Commission's €110 million fine against Facebook for having provided misleading information about the way the users' private data would be handled post-merger with WhatsApp, and Germany's investigation into Facebook's practice of forcing customers to agree to unfair terms about the way the company uses their data; See case M.8228, *Facebook/WhatsApp*, [2017] OJ C286/06; Commission decision of January 24, 2018, *Qualcomm*, case AT.40220; Judgment of October 6, 2015, *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650; Judgment of the Regional Court of Berlin of January 16, 2018, docket no. 16 O 341/15; Italian Competition Authority, Press release of November 29, 2018, Facebook, http://www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook, accessed on January 30, 2019; Bundeskartellampt, Decision of December 22, 2015, B-9-121/13, *Online hotel booking platforms*; Bundeskartellampt, Decision of October 22, 2015, Case B6-57/15, *Online dating platforms*; see also "Bundeskartellampt initiates abuse proceeding against Amazon," published on November 29, 2018, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/29_11_2018_Verfahrenseinleitung_Amazon.html.

4 Margrethe Vestager, extract from speech held at the *Conference on shaping Competition Policy in the era of Digitisation*, Brussels, January 17, 2019.

5 Case COMP/M.7217, *Facebook/WhatsApp*, [2014] OJ C417/4, para. 164.

sumers see it as a significant factor of quality."[6]

Recently, one of the world's most respected antitrust authorities – the German Federal Cartel Office ("FCO") – was also called to examine these issues in the context of proceedings launched in 2016 against Facebook for an alleged abuse of dominance. More specifically, in its preliminary legal assessment,[7] the FCO considered that Facebook is abusing its dominant position in the market for social networks through the imposition of "misleading" data protection policies to its users. Interestingly enough, the FCO seems to be more forward looking than the European Commission, underlining that **monitoring the data processing activities** of dominant companies is an **essential task of the competition authority**, which cannot be fulfilled by a data protection authority.[8] In its assessment of whether the company's terms and conditions on data processing are unfair, the competition authority does, however, take account of the legal principles of data protection laws by noting that "for this purpose, the Bundeskartellamt works closely with data protection authorities."[9]

The outcome of the German *Facebook* proceedings is of much interest for the development of both EU competition and data protection laws.[10] It will most likely set a precedent, since it is the first time that an infringement of data protection rules will be examined by a competition enforcer under abuse of dominance rules. Could this case therefore pave the way to a convergence between competition and data protection rules? Could this convergence result in a data sharing obligation imposed by competition enforcers on companies that are abusing their dominant position? Are we there yet? Or are we still at a stage where data protection is ***just*** a "dimension" of competition law in the tech sector?

To answer these questions, we will examine whether a synergy exists between EU competition law and EU data protection law, which would allow competition enforcers to impose data sharing – as an access remedy – in abuse of dominance cases. We will first briefly describe the two theories of harm upon which the FCO relied (in its preliminary legal assessment) and then analyze a potential data sharing remedy through the lens of both EU data protection and EU competition law.

II. ACCESS TO DATA – A POTENTIAL REMEDY IN A DOMINANCE ANTITRUST INVESTIGATION AGAINST TECH GIANTS?

A. The FCO's Theories of Harm in the Facebook *Case*

1. Users Lose Control over Their Personal Data

The FCO's first theory of harm focuses on the users' loss of control over their personal data: namely that "users are no longer able to control how their personal data is used."[11] In essence, the FCO takes issue with the fact that Facebook is collecting user data from third party websites when these websites implement a Facebook "like button" – even if the user is not using these services or has actively objected to web tracking.[12]

6 Commission, press release of December 6, 2016, IP/16/4284 in case COMP/M.8124, *Microsoft/LinkedIn*, [2016] C388.

7 Bundeskartellamt, "Background information on the Facebook proceeding," published on December 19, 2017, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6, accessed on January 30, 2019.

8 *Ibid.* question 3, page 2.

9 *Ibid.* question 3, page 2.

10 The German competition authority rendered the final decision on February 7, 2019. The decision was not yet published at the time of writing this article. In its press release, the German competition authority considered that Facebook's data processing terms, enabling the collection, merger and use of user data without valid consent, constituted an abuse of a dominant position justifying "far-reaching restrictions" on Facebook.

11 *Supra* note 7, question 7, page 4.

12 "If a third-party website has embedded Facebook products such as the 'like' button or a 'Facebook login' option or analytical services such as 'Facebook Analytics', data will be transmitted to Facebook via APIs the moment the user calls up that third party's website for the first time. These data can be merged with data from the user's Facebook account, even if the user has blocked web tracking in his browser or device settings." *Supra* note 7, "Background information on the Facebook proceeding," (2017), question 4, page 2.

This enables Facebook to collect personal data from users of these websites without their knowledge and even against their explicit will.[13] In the FCO's preliminary assessment, Facebook's terms and conditions in this regard are neither justified under data protection principles, nor are they appropriate under competition law standards. The FCO therefore found that Facebook violated the fundamental right to informational self-determination – which is enshrined in the German constitution[14] – of its users, which ultimately harms consumers.

It is interesting that "unfair" data protection policies are considered by the German competition enforcer as anticompetitive conduct/abuse of a dominant company occurring under the data protection sphere. One could claim that – in parallel with its antitrust enforcement – the FCO is actually also enforcing an infringement of Article 6 GDPR (Lawfulness of processing) under antitrust rules. In particular, Article 6(a) GDPR provides that "processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes."[15] While the FCO refrains from expressly analyzing whether users have given their *explicit consent* or not in its preliminary assessment, it implicitly indicates that users have not given Facebook their consent for the acquisition of their data from third party websites, since users have lost control over their data.[16]

The preliminary assessment of the FCO is silent on what constitutes specific and actual consumer harm resulting from the loss of control over users' data. It remains to be seen whether the FCO will build a solid bridge between a data protection concept – loss of control over a users' data – and the competition law concept of consumer harm.

If the European Commission prosecuted the same case under EU competition law, the Commission might allege that "misleading" data protection policies are a violation of Article 102(a) TFEU, an abuse of market dominance that imposes "unfair trading conditions." This could be seen as a consequence of the *Astra Zeneca* jurisprudence, where the European Court of Justice found the company's conduct consisting in "deliberate" and "consistent" "misleading representations" and "misleading information" to be an unfair trading condition,[17] although it is not clear that this case law would support this conclusion. If the Commission follows this approach, dominant online platforms competing for the acquisition of personal data and offering services that infringe data protection rules could face antitrust liability for the conduct insofar as it can be proved that this behavior in the market harms consumers.

2. Foreclosure of Facebook's Advertising Customers

The FCO's second theory of harm is only briefly described and relates to Facebook's potential foreclosure of its advertising customers. The German authority is worried that Facebook "is becoming more and more indispensable for advertising customers" and that "there is *also* potential for competitive harm on the side of the advertising customers who are faced with a dominant supplier of advertising space."[18] The word "also" in the abovementioned sentence may indicate that the foreclosure of advertising customers is not the focus of the FCO's investigation.

In other words, what the FCO seems to be saying is that Facebook is not only collecting user data from third party websites without valid consent, but with the help of this data it generates specific user profiles – that no other platform is able to generate – which in turn enable Facebook to improve its targeted advertising activities. Therefore, the FCO's theory may be that Facebook's leverage in a "targeted advertising market" is a consequence of its "unfair" data protection terms and conditions. Some problems that could arise from this theory relate to the fact that data might not be a rival good, there may be reasonable substitutes to data, a reasonable substitute may be available for purchase or even

13 "Facebook's users are oblivious as to which data from which sources are being merged to develop a detailed profile of them and their online activities. On account of the merging of the data, individual data gain a significance the user cannot foresee. Because of Facebook's market power users have no option to avoid the merging of their data, either. Facebook's merging of the data thus also constitutes a violation of the users' constitutionally protected right to informational self-determination." *Supra* note 7, "Background information on the Facebook proceeding," (2017), question 7, page 4.

14 The fundamental right to privacy is guaranteed by Art 1 in connection with Art 2 of the Grundgesetz.

15 Article 6(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

16 Contrary to the preliminary legal assessment, which did not mention the absence of user's consent, the President of the FCO stated in the press release accompanying the final (unpublished) decision that "The previous practice of combining all data in a Facebook user account, practically without any restriction, will now be subject to the voluntary consent given by the users. Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way." FCO press release "Bundeskartellamt prohibits Facebook from combining user data from different sources" available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3600108.

17 Judgment of December 6, 2012, *Astra Zeneca v. Commission*, C-457/10, EU:C:2012:770.

18 *Supra* note 7, question 7, page 4.

for free, data may be useless without a know-how with regards to processing and analyzing it, etc. If the FCO's final decision elaborates on this theory of harm, it will signal a growing intersection of competition law and data protection law.

Another question is whether the foreclosure of Facebook's customers who want to buy advertising space would be solved through an "access to data" remedy? Would this approach enable customers to enter the relevant market and to compete? In this sense, we will now analyze whether an "access to data" remedy in an abuse of dominance case would be possible under competition and data protection laws.

For the FCO's first theory of harm regarding data subjects' loss of control over their data, it is quite difficult to imagine a robust competition law remedy. We will therefore explore a potential remedy for the second theory of harm, i.e. foreclosure of Facebook's advertising customers. For this purpose, we will look at a potential "forced" data access from both competition law and data protection perspectives.

B. Competition Law Scrutiny of the "Access to Data" Remedy

While in the U.S. there is no competition law basis for a forced access to data remedy where a company owns or controls relevant data, in the EU this can be envisaged under the ''essential facility" doctrine.[19] This doctrine can provide a competition law remedy when a dominant company refuses to grant access to data, e.g. to an intellectual property right, as in the *IMS Health* case.[20]

The EU courts have held that a refusal to grant access to data – more specifically to license a proprietary IP right - is abusive if it is imposed by a dominant company and (i) the data is indispensable to compete; (ii) the refusal to provide access to data eliminates effective competition in a secondary market; (iii) it prevents the emergence of a new product or limits technical development; and (iv) it is not objectively justified.[21] Therefore, the threshold for EU competition authorities to impose a "forced" access to data remedy is very high. It is doubtful, however, whether these conditions are going to be met in the German *Facebook* case. If the conditions are met, it remains to be seen to which extent the FCO may be willing to impose such a forced access to data remedy to enable advertising customers to compete, given that its principal theory of harm was actually the loss of control over users' data.

Data as an indispensable input requires the existence of technical, legal, or even economic obstacles capable of making duplication impossible, or even unreasonably difficult.[22] It would therefore be necessary for the FCO to establish, at least, that it is not economically viable for Facebook's advertising customers to create an alternative facility at a scale comparable to that of Facebook. One could therefore argue that for Facebook's advertising customers, it is impossible to recreate the amount of data that Facebook possesses, given that Facebook has gathered such specific information (also from third-party websites) that it can divide its users in no less than 29,000 categories.[23]

The second condition would involve the fact that Facebook's refusal to supply access to data to advertising customers would eliminate effective competition from a secondary market, where Facebook is also present. In other words, if Facebook refuses to supply data to a customer that is advertising electronics, only in the situation in which Facebook would also be active in the electronics market and would try to reserve this market for itself by refusing to deal, would this be anticompetitive. This means that, under the current interpretation of case-law, Facebook can legitimately refuse to give access to its data to advertising customers and prevent them from competing in markets in which Facebook itself is not present (yet).

A forced data sharing remedy would therefore fail to satisfy the second condition of the essential facilities doctrine. However, one needs to bear in mind that these conditions are "created" through jurisprudence of the EU courts and are not set in stone.

---

19 See Graef I., "EU Competition Law, Data Protection and Online Platforms," International Competition Law Series, Wolters Kluwer, 2016. See also Supreme Court of the United States, case 02-682, *Verizon Communications v. Trinko LLP*, where US Supreme Court held that a monopolist's unilateral refusal to cooperate with a rival is lawful where there is no history of a prior course of dealing.

20 Judgment of April 29, 2004, *IMS Health*, C-418/01, EU:C:2004:257.

21 *Ibid*. para. 38; Judgment of September 17, 2007, *Microsoft v. Commission*, T-201/04, ECLI:EU:T:2007:289, paras. 330–336.

22 Judgment of November 26, 1998, *Bronner*, C-7/97, EU:C:1998:569, para. 44.

23 Graef I. & Prüfer J. (2018), "Mandated data sharing is a necessity in specific sectors," Economisch Statistische Berichten, 103(4763), 298-301.

The third condition requires that the refusal to give access to data prevents the development of a new product – but this condition has only been applied for refusals to license intellectual property rights.[24] It may make no sense to apply this condition in the present case, because advertising customers want to have access to Facebook's data specifically because they want to sell their products.

As for the forth condition, Facebook may invoke an objective justification to offset an alleged refusal to give access to its data to advertising customers. Objective justifications that were accepted by EU courts were capacity restraints in supply (*Commercial Solvents*),[25] or improper commercial behavior of the customer (*United Brands*).[26] The question also arises whether a forced data sharing remedy could also be anticompetitive in and of itself if the data reveals competitively sensitive information from the data provider.

Assuming that none of these could apply in the present case, Facebook may potentially invoke data protection law to offset the claim.

In this sense it is interesting to note a recent case enforced by the French Competition Authority, where it found that a company was dominant and ordered it to disclose customer data to its competitors, since the data was strictly necessary to ensure that competitors could effectively approach customers and compete.[27] Nonetheless, it also imposed an obligation on the dominant company to introduce a system on the basis of which its customers could be informed of such transfer and have the possibility to oppose it.[28] In other words, while the French Competition Authority imposed a forced access to data as a competition law interim remedy, it also ensured that there was an opt-out on data protection grounds.

Therefore, in this context we will discuss whether, at the EU level, data protection law could constitute an objective justification for offsetting a potential "access to data" remedy.

C. Data Protection Scrutiny of the "Access to Data Remedy"

Assuming that a forced data access remedy would be possible from a competition law perspective, could this be trumped by data protection law, i.e. the GDPR? If a competition authority would impose upon a dominant player an obligation to share part of the data it controls with its customers or competitors, could this company defend itself by claiming that this would run against its obligations under the GDPR? The answer is not clear cut.

The dominant company under investigation, i.e. the potential data provider, could argue that a **forced data sharing** means that personal data will not be processed fairly and in a transparent manner in relation to the data subject, and would therefore **run against its obligations under Article 5(a) GDPR** ("lawfulness, fairness, and transparency principle"). In addition, according to Article 15 GDPR, the dominant company would have to inform data subjects that their personal data is being transferred to another company, to which they have not given their consent.

It is also important to note that the GDPR does not contain any explicit provisions for a potential "forced" personal data transfer mechanism between two private companies, as a consequence of imposing such a remedy on a dominant company following a competition law investigation. Arguably, the company to which the data is being transferred, i.e. the data seeker (a customer or a competitor),[29] would not have any legal basis for processing the personal data, so it would need to seek consent of the respective data subjects, which would be a very cumbersome task. Contrary to the alleged dominant player, i.e. the original data controller, who is forced by competition authorities to transfer data, the data seeker would not be able to claim that "processing is necessary for compliance with a *legal obligation* to which it is subject" (Article 6(c) GDPR), because it would not be under any legal obligation to process the data.

24 Judgment of September 17, 2007, *Microsoft v. Commission*, T-201/04, ECLI:EU:T:2007:289.

25 Judgment of March 6, 1974, *Commercial Solvents v. Commission*, joined cases C-6/73, C-7/73, ECLI:EU:C:1974:18.

26 Judgment of February 14, 1978, *United Brands v. Commission*, C-27/76, ECLI:EU:C:1978:22.

27 Autorité de la concurrence (Paris), *GDF Suez/Direct Energie*, Decision n° 14-MC-02, September 9, 2014

28 *Ibid*. para. 294.

29 In our case, the "data seekers" would be Facebook's advertising customers.

On the contrary, we are assuming that it is the customer/competitor who wanted to get access to the data in the first place through his voluntary will. In this context, a customer/competitor who would want to get access to data withheld by a dominant player may argue that a valid legal basis for the data processing constitutes "his legitimate interest" of promoting his business. This would, however, be a far-fetched interpretation of Article 6(f) GDPR, which may provide an adequate legal basis for a lawful processing for the data seeker. Moreover, it is also unclear which role the data seeker will play in this scenario, i.e. whether it will be considered to be a sole controller or a joint controller. In sum, one could therefore argue that the GDPR is probably ill-equipped to support a potential "forced" data sharing remedy in an abuse of dominance case.

III. CONCLUSION

In today's digital economy, personal data has economic value and is an important parameter of competition. The dynamics of the online world seem to have caught some regulatory and legislative authorities off guard. Today's reality is that competition and data protection law increasingly intersect but Europe's brand-new data protection law, the GDPR, lacks any explicit provisions for a potential "forced" mechanism to provide access to data following the imposition of such an obligation by a competition authority.

Competition authorities seem to be enforcing data protection standards in antitrust cases, but data protection authorities may apply different standards. This may lead to additional complexity of a regulatory framework that is already quite burdensome for businesses. The FCO's decision in the German *Facebook* case is eagerly awaited. It may set an important precedent, since it is the first time that an infringement of data protection rules will be examined by a competition enforcer under abuse of dominance rules. The case makes clear that from now on companies will need to bear in mind that enforcing "*unfair*" data processing policies may potentially violate both competition law provisions as well as European data protection laws.

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.