Organisation for Economic Co-operation and Development

DAF/COMP/WD(2020)40

Unclassified

English - Or. English

3 June 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Consumer data rights and competition – Note by the European Union

12 June 2020

This document reproduces a written contribution from the European Union submitted for Item 3 of the 133rd OECD Competition Committee meeting on 10-16 June 2020.

More documents related to this discussion can be found at
http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm

Please contact Ms Anna BARKER if you have questions about this document.
[Email: Anna.BARKER@oecd.org]

JT03462464

European Union

1. Consumer data in today's marketplace

1.1. The collection and use of consumer data

1. With the proliferation of online services and technological advances exponentially increasing the ability to store, process and analyse data, the collection and use of personal data generated by individual consumers as they use the internet has become a cornerstone of the digital economy. Businesses are hungry for the data of their customers because the data enables them to understand what consumers want and how they want it. Consumer data can be used to tailor and target products and services (including advertising), understand how products can be improved and discover the need and demand for new products and services.

2. The internet as we know it today supports the collection of a wide range of consumer personal data. Consumers generate personal data whenever they register on a new website or sign up for a new service. They also generate large amounts of varied personal data in a 'passive' way, for example by shopping online (transactional data), searching or otherwise using content on the web (browsing behaviour), using a smartphone (location and app usage data) and adding contacts or communicating on social media (the so-called 'social graph').

3. Increasingly, a wide range of consumer devices fitted with sensors and connected to the Internet of Things (IoT) such as digital voice assistants, home appliances, smart watches and other 'wearables' and even passenger cars, are becoming additional channels for the creation of personal data related to the usage of these products and its transfer from the consumer to businesses.

4. Firms collect data from consumers both on a first-party basis (via the use of the firms' own products or services) and, often, as third parties without a direct relationship to the consumer. Technologies used to track the online behaviour of consumers include first-party and third-party cookies[1] as well as lesser known techniques such as pixels and 'fingerprinting'.[2] Data from various sources that can be attributed to specific consumers by means of such techniques are combined and analysed to build richer, more complete profiles of user behaviour encompassing browsing and purchasing habits, interests, political beliefs and others. The creation of such detailed user profiles enables the segmentation of consumer groups for targeting purposes along many different parameters.

[1] 'Cookies' refer to bits of text that are placed on a user's browser by web domains visited by that user, enabling that domain to track the user's activity and 'remember' the user on subsequent visits. First-party cookies refer to cookies placed by the publisher of the website being visited; third-party cookies refer to those placed on the browser by other entities with the first party's permission. The placing of cookies on a user's device for purposes of online tracking is in principle subject to the informed, freely given consent of the user under Article 5(3) of the 'e-privacy Directive' (Directive 2002/58/EC).

[2] Pixels are bits of code placed on a website that send information on a user's activity to servers. Unlike cookies, they are not stored on the user's browsers and cannot be disabled by users. Fingerprinting refers to techniques for collecting information about the software and hardware of a computing device for purposes of identification of the user.

5. While first party data collectors may analyse customer behaviour on their own properties, there are also specialised third party data analytics providers that perform this as a service to publishers or, indeed, trade in consumer datasets.

6. Large platforms offering diverse consumer-facing services are particularly well-placed to collect rich and diverse first-party consumer data from their services. Many platforms collect data on consumer characteristics, activity such as searches and browsing behaviour, content created and shared and location via the users' device information. The type and amount of data varies depending on factors such as whether a user is logged in to a particular website or environment when using the service, whether the use is via a browser or mobile app, or whether the device is a mobile or a 'static' device.

7. Two well-known platforms in particular have business models that are largely dependent on the collection of consumer data and its use in the provision of online advertising services to advertisers. Google collects first-party data through the many Google consumer-facing services (search, Google Maps, YouTube, Gmail, etc.) offered at a monetary price of zero, as well as through the Android operating system for mobile devices. The data is used for a number of purposes according to Google's privacy policy, including improvement of Google services and the development of new services, but also for the provision of personalised services including content (e.g. YouTube viewing recommendations) and ads.[3]

8. Facebook collects data from its three main consumer-facing services: the Facebook social network and its affiliated Messenger instant messaging service; Instagram; and WhatsApp. Like the majority of social networking and electronic messaging services, the Facebook group monetises its services not by charging fees to users, but rather primarily by means of advertising. Facebook collects a wide variety of first-party data including usage, device information, social information including connections and communications. The data is used for personalisation of products, content and ads, facial recognition and the provision of measurement, analytics and other services to advertisers and other partners.[4]

9. Both groups also collect large amounts of data from consumers' use of third-party products and services via the extensive use of cookies, log-ins, pixels, the provision of advertising and analytics services and other means. Although, as mentioned above, other 'Big Tech' platforms such as Amazon, Apple or Microsoft collect significant amounts of consumer data, much of the worldwide focus of regulators in relation to data collection practices has concentrated on Google and Facebook due to their powerful roles in online advertising and their focus on the delivery of personalised online content.[5]

1.2. Consumers' perceptions of commercial data collection and online tracking

10. In parallel with the increasing commercial focus on the collection and use of consumer data fuelled by the rapid and continuing expansion in commercial and social

[3] See Google's privacy policy, available at https://policies.google.com/privacy?hl=en-US, accessed on 15 April 2020.

[4] See Facebook's Data Policy, available at https://www.facebook.com/policy.php, accessed on 15 April 2020.

[5] See, e.g., the report from the Digital Platforms Inquiry of the Australian Competition and Consumer Commission, the interim report of the UK's Competition and Markets Authority market study on online platforms and digital advertising and the report on the online advertising market inquiry by the French Autorité de Concurrence.

interactions carried out online, the topic of online privacy and data security appears to be gaining increasing prominence within civil society[6], the media[7] and the public.

11. In the latter part of the previous decade, the public in Europe and elsewhere became more aware and concerned about how personal data was collected and used online. Recent Eurobarometer public opinion surveys have indicated, inter alia, that majorities of EU consumers experience pervasive targeted online advertising as an irritant.[8] In a mid-2019 survey on attitudes and awareness towards the EU's General Data Protection Regulation (GDPR), majorities of respondents reported that they at least partially read privacy statements online and that they have at least tried to change the default privacy settings on a social network to which they belong. Further, although two-thirds of respondents claimed they felt they had at least partial control over the data they provided online, a majority (51%) of all respondents felt that this control was only partial and 30% felt they had no control at all. Out of those who felt they had only partial or no control, a majority (62%) reported being concerned about this.[9]

12. The GDPR survey mentioned above further showed that, among consumers who only partially read or did not read privacy policies, majorities reported finding them too long to read whilst significant percentages reported finding them unclear or difficult to understand. Some respondents also reported that the fact that a website has a privacy policy at all is sufficient, and that they trust social networks to set appropriate privacy settings, indicating that trust in relation to data protection standards is an important factor for at least some consumers.[10]

13. The significant body of academic and research literature concerning consumer attitudes towards privacy and data protection is mixed and evolving. The term 'privacy paradox' has been used to refer to the perceived contradiction between surveys that consistently show that large numbers of consumers claim to be concerned about their online privacy and the reality that they nevertheless make little effort to protect their personal data.[11] Some observers have advanced the view that easy access to free online services is more important to consumers than any privacy risk and that, therefore, competition authorities should not concern themselves at all with privacy policies and data protection standards. Other research focuses on surveys showing that a growing number of consumers not only care about the privacy and security of their data, but also that these are important factors influencing their buying decisions and their online behaviour. Increasing numbers of individuals have already taken action to protect their privacy, for example by switching companies or providers because of their data policies or data sharing practices. This "privacy active" segment of the population has been identified as being mostly people

[6] See, e.g., Amnesty International's report "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights", published 21 November 2019.

[7] See, e.g. the New York Times' Privacy Project, available at https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html, accessed on 15 April 2020.

[8] Special Eurobarometer survey no. 447 on "Online platforms", June 2016, page 62.

[9] Special Eurobarometer survey no. 487a on "The General Data Protection Regulation", June 2019, pages 3-4, 34, 39.

[10] Idem, page 51.

[11] See, e.g., S. Kokolakis, "Privacy attitudes and privacy behaviours: A review of current research on the privacy paradox phenomenon", Computers & Security 64 (2017), pages 122-134; S. Barth & M. de Jong, "The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behaviour – a systematic literature review", Telematics & Informatics Volume 47, Issue 7, November 2017, pages 1038-1058.

under the age of 45 who do a large proportion of their shopping online compared to the rest of the population[12].

14. Notwithstanding this continuing debate, the survey results discussed above, together with the undeniable intensified focus on issues of privacy and data protection in Europe and globally in particular since the advent of the GDPR, suggest that, at a general level, consumers in the EU are increasingly interested in how their personal data are used by undertakings. Market investigations in many of the cases outlined below in Part 3.1.1 broadly support the view that significant numbers of consumers care about the protection of their personal data, and by extension that competition authorities should take privacy standards into account in cases where these are relevant parameters of quality, innovation or choice.

2. Consumer data rights in the EU

2.1. The GDPR legal framework

15. Article 8 of the EU Charter of Fundamental Rights defines the protection of personal data as a fundamental right and provides that personal data must be processed fairly and for defined purposes, and must be based on the consent of the person concerned or some other legitimate basis set forth by law. The Charter further provides that an independent authority must be competent to control compliance with the relevant rules.

16. The GDPR has been the main data protection legislation in the EU since it became applicable on 25 May 2018. Its provisions set out the framework for lawful and fair processing, the overarching data protection principles applicable in the EU, the rights enjoyed by data subjects and the obligations incumbent upon economic operators when processing personal data. Importantly, it also empowers the data protection authorities of the Member States (DPAs) to impose sanctions, including fines, on companies violating its provisions, including in cross-border cases under a cooperation mechanism under the auspices of the European Data Protection Board. The possibility for data subjects to mandate non-profit organisations to pursue collective actions in their name is also guaranteed (Article 80). The future Directive on representative actions for the protection of the collective interests of consumers[13] will further strengthen the framework for representative actions, including in the field of data protection. Citizens, consumer organisations and others have made extensive use of the ability to file complaints with the DPAs, many of which are still pending and involve data collection practices of the kinds described in part 1 above.

17. Personal data can only be lawfully processed under the GDPR pursuant to at least one of the six valid legal bases set forth in its Article 6. In the context of consumer data used for commercial purposes, the three most relevant legal bases are the following:

- ***Consent (Article 6(1)(a))*:** this must be expressed by means of a freely given, fully informed, specific and unambiguous statement or affirmative action signifying agreement to the specific processing. Consent must be made on an 'opt-in' and not 'opt-out' basis and must be as easy to withdraw as it was to give. Pursuant to Article 7(4) GDPR, when assessing if consent is freely given, utmost account must be taken

[12] See, e.g., Consumer Privacy Survey by Cisco, Cybersecurity Series 2019, available at https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf.

[13] COM/2018/0184 final - 2018/089 (COD).

of whether the performance of a contract, including the provision of a service, is made conditional on consent to the processing of personal data that is not necessary for the performance of the contract.

- ***Contract (Article 6(1)(b))*:** this constitutes a valid legal basis to the extent that the processing is necessary for the performance of a contract with a customer. An example of this is when a customer must submit personal data in the form of a name, address, mailing address, etc., when making an online purchase. Processing of personal data that goes beyond what is necessary to fulfil the purpose of the contract is not covered by this legal basis and in this situation the undertaking (the data controller) must rely on another legal basis, e.g., consent.
- ***Legitimate interests of the data controller (Article 6(1)(f))*:** data controllers can rely on this legal basis pursuant to a three-part balancing exercise involving an assessment of whether the interests and fundamental rights and freedoms of the data controller override those of the data subject in relation to the processing.

18. The most appropriate legal basis in a specific case depends on the nature and purpose of the processing and the relationship between the data controller and the data subject. In the context of behavioural advertising, data protection authorities in the EU have generally taken the view that consent is the only possible valid legal basis. Legitimate interest has been deemed in principle not appropriate in relation to the intensive collection and other processing of personal data used in the serving of personalised advertising, as the interest of the controller is unlikely to outweigh the data protection interests of the consumer. Accordingly, the consent of the data subject normally must be secured in order to process personal data for the purposes of providing behavioural advertising and, in many cases, personalised digital content.[14]

19. The GDPR grants certain specific rights to data subjects, including the right to access one's personal data (Article 15); the right to rectify inaccurate personal data (Article 16); the so-called 'right to be forgotten' (Article 17); the right to data portability (Article 20); the right to object to specific processing operations (Article 21); and the right not to be subject to automated decision-making, including personal profiling, subject to exceptions (Article 22). In furtherance of the exercise of these rights, the GDPR obligates economic operators to provide specific information to data subjects (Articles 13 and 14) in a concise, transparent, intelligible and easily accessible form (Article 12).

20. Among the rights of the data subjects as such, the novel right of data portability is of particular importance from the point of view of competition.

2.2. The right to data portability (GDPR)

21. Article 20 GDPR provides that "[t]he data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit

[14] See European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019; Opinion 06/2014 of the Article 29 Working Party on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014 (referring to the Data Protection Directive, predecessor to the GDPR). Article 9 GDPR further states that processing of certain special categories of personal data, for example data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health and data concerning a person's sex life or sexual orientation requires explicit consent of the data subject or it is prohibited, subject to certain exceptions which would normally not apply in the context of consumer online services.

those data to another controller without hindrance from the controller to which the personal data have been provided." The right applies when the processing was carried out by automated means and the legal basis for the processing was either consent of the data subject (Article 6(1)(a)) or the performance of a contract (Article 6(1)(b)). Article 20(2) further specifies that, where technically feasible, the data subject shall have the right to have the personal data transmitted directly from one controller to another.

22. The data portability provision in the GDPR is first and foremost a means of further strengthening the data subject's control over his or her data[15], but its relevance for competition between economic operators (data controllers) is clear. Article 20 facilitates switching between and among providers of data-driven services, thereby preventing data subjects from being locked in to specific service providers on account of the data held by those providers.[16] In the *Sanofi/Google/DMI JV* merger case, the Commission investigated whether the creation of a joint venture offering data-related services to diabetes patients would be able to lock in patients by preventing them from porting data to alternative platforms. In concluding that the risk of a lock-in effect was unlikely to materialise in the foreseeable future, the Commission noted the existence of the data portability provision in the draft GDPR, as well as the fact that alternative providers seemed capable of establishing themselves before the joint venture could come to market.[17]

23. The right applies to personal data *provided* by the data subject. This clearly covers data actively and knowingly provided, such as mailing address, electronic contact details, username, age and other information that may be provided when registering for a service. It also, however, covers 'observed data' provided by the data subject by virtue of the use of the service or device. Such observed data may include search history, traffic data or location data, or other raw data such as the heartbeat tracked by a wearable device. The right to portability notably does not cover 'inferred data' or 'derived data' created by the data controller on the basis of the data provided by the data subject, such as the results of algorithmic analysis or other assessments performed on the data provided. Thus, data is covered by Article 20 if it relates to the data subject activity or results from the observation of an individual's behaviour, but not if it constitutes subsequent analysis of that behaviour.

24. Due to the 'youth' of the right as a statutory provision, it is pre-mature to draw definite conclusions as to its impact. Technological solutions still need to be developed to fully ensure the effective exercise of this right, as reflected in the GDPR itself, which states that "*[d]ata controllers should be encouraged to develop interoperable formats that enable data portability*." The contribution of a multistakeholder expert group to the Commission's stock-taking exercise of June 2019 on one year of GDPR application noted certain initiatives in the private sector aiming to develop tools enabling consumers to exercise this right, but also reported certain areas for improvement. These included the need for better explanation of the right to data subjects and the development of more practical formats with which to exercise the right.[18] Unlocking the full potential of this right to empower

[15] GDPR, recital 68.

[16] See Article 29 Working Party Guidelines on the right to data portability, as last revised and adopted on 5 April 2017, page 4; "Competition policy for the digital era", a report by Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer (special advisors to Margrethe Vestager), 2019, page 81.

[17] Case COMP/M.7813 *Sanofi/Google/DMI JV*, decision of 23 February 2016, paragraph 69.

[18] Contribution from the Multistakeholder expert group to the stock-taking exercise of June 2019 on one year of GDPR application, Multistakeholder Expert Group to support the application of Regulation(EU) 2016/679, Report of 13 June 2019, available at https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf.

consumers going forward should be a priority, in particular since, given the increasing use of complex IoT devices and applications, more and more data are generated by consumers in scenarios where risks of discrimination, unfair practices and 'lock-in' effects may be present.

2.3. Data access rights in other EU legislative instruments

25. In specific sectors, the EU has adopted legislation mandating certain data sharing or access obligations in order to open up the offering of certain services to competition. For example, the Payment Services Directive II ('PSD2') obligates banks offering online access to accounts to make customer account data available through secure channels to approved third parties upon the explicit consent of the customer. This enables third parties to offer specific innovative payments solutions to customers such as payment initiation services and account information services.[19]

26. Further sector-specific data access obligations in EU law addressing identified market failures exist in areas including automotive,[20] smart metering information,[21] electricity network data,[22] or intelligent transport systems.[23]

2.4. 'Enhanced' data portability in the Commission's data strategy

27. The Commission's communication on "A European strategy for data" published in February 2020 explores future potential measures to empower individuals with respect to their data.[24] The communication ("the data strategy") proposes, among many other potential instruments, a Data Act featuring provisions intended to further support individuals in relation to the enforcement of their rights with respect to the use of the personal data they generate, in particular by providing tools and means to exert more granular control over what is done with their data. Such an act could include provisions enhancing the right to data portability under Article 20 of the GDPR. This could include giving individuals more control over who can access and use machine-generated data, for example by imposing stricter requirements on interfaces for real-time data access and making machine-readable formats compulsory for data from certain products and services, such as data coming from the use of smart home appliances or wearables.

28. The data strategy notes that the Commission will also consider adopting rules governing providers of personal data apps or novel data intermediaries such as 'personal data spaces'. Data portability is also a primary concern in the data strategy's plans for a common European health data space, where the Commission intends to take measures to strengthen citizens' access to health data and the portability of this data across borders, thereby promoting competition by tackling barriers to cross-border health services and products. Like PSD2, these potential future instruments are motivated by considerations of

[19] Directive 2015/2366; see also Commission FAQ, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555, accessed on 20 April 2020.

[20] Regulation 715/2007 as amended by Regulation 595/2009.

[21] Directive 2019/944 for electricity, Directive 2009/73/EC for gas meters.

[22] Commission Regulation (EU) 2017/1485, Commission Regulation (EU) 2015/703.

[23] Directive 2010/40/EU.

[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", 19 February 2020 COM (2020) 66 final.

consumer and innovation empowerment with the aim of preventing 'lock-in' effects and unfair practices that can harm consumers.[25]

3. Theories of harm and challenges at the intersection of competition enforcement and consumer data rights

3.1. Theories of harm in competition enforcement

29. As noted in a Commission submission to a previous OECD roundtable, compliance with the GDPR and the regulation of data protection standards is not, as such a matter for competition law enforcement.[26] These matters are specifically addressed by data protection law as enforced by the DPAs of the EU Member States, empowered to impose sanctions including fines since the GDPR became applicable on 25 May 2018. However, in instances where the processing of personal data and the standards of data protection are relevant to the competitive process, there is a case for competition enforcement and competition authorities may take these aspects into account, in particular as relevant non-price aspects of competition, such as product quality, innovation or consumer choice.

3.1.1. Merger control

30. The Commission has reviewed numerous mergers in recent years between undertakings with business models involving intensive collection and use of consumer (personal) data.[27] In this context, the Commission has investigated two principal theories of harm: (i) that the concentration of datasets held by the merging parties could act as a barrier to entry or expansion, or as a means to foreclose rivals, and (ii) that the transaction could cause a degradation of the quality of data protection, which is deemed an important parameter of competition.

31. In relation to the former, the existence of robust data protection laws may, in the Commission's view in previous cases, serve to remove competition concerns that may otherwise arise in relation to the combination and use of diverse types of consumer data. Thus, in its 2012 review of *Telefonica UK/Vodafone UK/Everything Everywhere*, the Commission looked into the issue of foreclosure of competing providers of targeted advertising services. The potential concern was that the joint venture offering various mobile commerce services in the UK could combine personal information, location data, response data, social behaviour data and browsing data to develop a unique database for the purposes of advertising which no competitor would be able to replicate. The Commission's evaluation revealed that information available to the joint venture company was also available to existing and new market players which were already using it to provide targeted advertising. Therefore, since many other strong competitors offered comparable solutions, they would not be foreclosed from an essential input and the joint venture company would not have a negative effect on competition. Additionally, the

[25] Idem, page 10.

[26] DAF/COMP/WD(2018)135, Quality Considerations in the zero-price economy – Note by the European Union, October 2018.

[27] An early, much-discussed case in this regard is the acquisition of DoubleClick by Google, reviewed by the Commission in 2008.

Commission noted that the joint venture would in principle be constrained by data protection laws requiring customers to opt-in to the relevant forms of data processing.[28]

32. In *Verizon/Yahoo!*, the Commission examined whether the combination of the two datasets of the firms would increase the merged entity's market power or create barriers to entry in the market of online advertising. The Commission again concluded that the data protection rules (namely the GDPR that was to become applicable two years after this decision) would limit the parties' ability to use the personal data that they collected. Additionally, there would continue to be a large amount of internet user data that were valuable for advertising purposes and that were not within the exclusive control of the merged entity. Finally, the parties were small market players in online advertising. Finally, the data collected by Yahoo and Verizon could not be characterised as unique.[29]

33. A potential concern in *Apple/Shazam* was that Apple would gain access to "commercially sensitive data" of its music streaming rivals, thus putting its competitors at a competitive disadvantage. The data collected by Shazam allowed it to identify if the user already had a music streaming app installed and if they were a premium or "freemium" subscriber, which Apple could use in its marketing campaign to target competitors' "freemium" subscribers. The Commission assessed the legal and contractual limitations to the use of customers' data and concluded that, while Apple could have the ability to use Shazam's data in this way, it was unclear whether it had an incentive to do so and, in any case, it was unlikely to have a negative impact on effective competition because: (i) rivals would continue to have access to similar information through apps other than Shazam (e.g., Facebook, Google, and Twitter); (ii) Apple's ability to target rivals' customers would not materially increase post-transaction; (iii) in the steadily growing market for music streaming services, providers focus on attracting new customers rather than convincing rivals' subscribers to switch; and (iv) Apple's internal documents showed that the transaction would have a low impact on Apple Music's customer acquisition rate.[30]

34. An additional concern of the Commission was whether Shazam's data would be so useful for improving Apple Music's functionality as to put rival streaming services at a competitive disadvantage. In this case, the Commission analysed Shazam's data to assess whether other datasets were truly comparable. The Commission used an analytical framework based on the concept of the "Four V's": it analysed how Shazam's user data compared to other datasets available in the market in terms of their variety, velocity, volume, and value. This analysis revealed that even if Apple were to restrict access to Shazam's data, it would not harm rival music streaming providers.[31]

35. In its review of Facebook's acquisition of WhatsApp, the Commission analysed whether data concentration was likely to strengthen Facebook's position in the online advertising market. It explicitly stated that: "*Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*."[32] The Commission noted that WhatsApp did not collect any user data that are valuable for advertising purposes and thus concluded that the transaction would not have increased the amount of data potentially available to Facebook

[28] Case COMP/M.6314 – *Telefónica UK/Vodafone UK/Everything Everywhere/JV*, decision of 4 September 2012.

[29] Case COMP/M.8180 *Verizon/Yahoo!*, decision of 21 December 2016.

[30] Case COMP/M.8788 *Apple/Shazam*, decision of 6 September 2018.

[31] Idem, paragraphs 317-329.

[32] Case COMP/M.7217 *Facebook/WhatsApp,* decision of 19 November 2014*,* paragraph 164.

for advertising purposes. The Commission cleared the merger, concluding – among other things - that: i) regardless of whether the merged entity would introduce advertising on WhatsApp, there would continue to be a sufficient number of other actual and potential competitors equally well placed to offer targeted advertising;[33] and ii) regardless of whether the merged entity would start using WhatsApp user data to improve targeted advertising on Facebook's social network, there would continue to be a large amount of Internet user data outside of Facebook's control that would be useful for online advertising.[34] The greater privacy protection offered by WhatsApp compared with Facebook was one of the factors leading the Commission to conclude that the parties were not close competitors, and consumers' increasing focus on privacy meant that Facebook would be unlikely to retract WhatsApp's plans to add end-to-end encryption and introduce targeted advertising into WhatsApp.[35]

36. In *Microsoft/LinkedIn*, the Commission assessed whether the combination of Microsoft's and LinkedIn's datasets would increase the market power of the merged entity or raise barriers to entry. It noted that applicable data protection rules (including GDPR) may limit Microsoft's ability to use its users' personal data. In any event, the Commission dismissed these concerns because (i) Microsoft and LinkedIn did not make available their data to third parties for advertising purposes; (ii) there would continue to be a large amount of data useful for advertising purposes, outside of Microsoft's control; and (iii) the parties were small players in online advertising.[36]

37. Importantly, however, in this investigation the Commission acknowledged that privacy was a "driver of customer choice" and "an important parameter of competition" and that it was possible for companies to compete on the basis of privacy policy 'to the extent that consumers see it as a significant factor of quality.'[37] The Commission's market investigation further led it to recognise data protection standards as an important parameter of competition in the market for professional social networks. The merger raised the concern that Microsoft's integration of LinkedIn features could foreclose competitors to LinkedIn such as Xing, a professional social network active in Germany and Austria. The Commission found that Xing offered a higher level of privacy protection to users than LinkedIn, particularly in relation to the choice architecture it used to obtain user consent for the processing of personal data as well as the fact that, when revising its data policy, it allowed users to retain use of the services without accepting all of the new changes. The potential foreclosure effect would therefore restrict consumer choice in relation to an important parameter of competition. In order to resolve this concern, Microsoft offered commitments to resolve the foreclosure concerns and hence preclude any privacy-related harms.[38]

[33] Idem, paragraph 179.

[34] Idem, para 189.

[35] As of April 2020, WhatsApp maintains that its communications are end-to-end encrypted. In 2019, Facebook announced plans to integrate WhatsApp with its Facebook Messenger instant messaging application and the messaging function on Instagram and use end-to-end encryption on the integrated product, meaning messages could only be read by the sender and recipient. This process is not yet complete.

[36] Case COMP/M.8124 *Microsoft/LinkedIn*, decision of 6 December 2016, paragraphs 167-181.

[37] Idem, paragraph 350.

[38] Ibid.

3.1.2. Antitrust

38. In the field of merger enforcement, competition authorities have built up a significant amount of experience in the last decade in the process of reviewing transactions such as those described above. By comparison, there is to date a relative paucity of antitrust cases in which data protection plays a prominent role, either in respect of the theory of harm or in relation to a remedy.

39. There is a wealth of recent literature proposing various theories of harm arising from the collection and use of personal data, in particular by dominant undertakings.[39] It has been proposed, *inter alia*, that a reduction in the level of data and privacy protection offered to users could constitute an exploitative abuse in the form of unfair terms and conditions, or under a theory of excessive pricing in which a reduction in the quality of data protection becomes 'excessive' as a quality-adjusted price 'paid' by the customer in the form of data captured by the dominant firm.[40]

40. The best-known example of such a case of exploitative abuse is the highly publicised 2019 decision by Germany's Bundeskartellamt against Facebook, finding an abuse of dominance under German law (and not in application of Article 102 TFEU) in the social media market in respect of the excessive collection by Facebook of consumer data outside the Facebook social network itself. The Bundeskartellamt found that Facebook had not obtained meaningful consent to collect and combine such data and had forced abusive 'take-it-or-leave-it' terms on users which resulted in extensive data collection that entrenched its dominance. Facebook's request for interim measures against the decision to the Higher Regional Court in Dusseldorf was successful, temporarily relieving Facebook of the obligation to comply with the decision, subject to ongoing appeals. The case has yet to reach a final resolution. No other similar case has yet surfaced.

41. Regardless of the final outcome of the German Facebook case, it is apparent that exploitative theories of harm are challenging in relation to defining what constitutes an excessive or unfair level of data collection or use from a consumer's point of view, as well as in establishing the necessary link between such data practices and abusive conduct in the sense of competition enforcement. In the EU, since the GDPR enforcement system is fully capable of sanctioning practices in violation of the standards for gaining informed consent and the rules against bundling processing operations, the case for competition enforcement in relation to these practices arguably needs to be particularly robust.

42. The use of consumer data may also be relevant for exclusionary theories of harm. Foreclosure could occur, for example, where a dominant firm engages in exclusionary conduct that restricts rivals' access to consumer data (provided consumer data is an important input), or that raises rivals' costs or erects barriers to entry or expansion, for example by engaging in tying and bundling with the aim of entrenching its dominance or

[39] It should be noted that although most relevant theories of harm involve abuses of dominance (Article 102 TFEU), collusion on the level of privacy protection offered to consumers or agreements to provide services at zero-price in order to maximise the collection and use of consumer data could in principle be caught by the rules on anticompetitive agreements and concerted practices (Article 101 TFEU).

[40] See, e.g. V. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", (2020) 57 Common Market Law Review, pages 161–189; N. Economides & I. Lianos, "Antitrust and Restrictions on Privacy in the Digital Economy", NET Institute Working Paper No. 20-03. Note again that in this scenario, the monetary price actually charged to the consumer is typically zero, with the return on the data collected made by charging advertisers on the other side of the platform.

leveraging it into adjacent markets.[41] Both the UK and French authorities have, in the recent past, required retail energy businesses to make their customers' energy data available to competitors, provided consumers were given the right to opt-out of such data access remedies.

3.2. Challenges at the intersection of competition law and data protection standards

43. The relationship between competition and data protection laws, and how questions surrounding data protection should be incorporated into competition assessments, is relatively new but has sparked vigorous debate. An extensive body of academic literature already exists, but enforcement decisions developing theories and creating precedents in this area are still relatively rare, particularly in the field of antitrust.

44. Enforcement authorities will have to grapple with certain analytical and empirical challenges when investigating cases involving firms with consumer data-driven business models, as acknowledged in the OECD's comprehensive background note.[42] These include (i) identifying cases where the accumulation of personal data in the hands of undertakings with market power can give rise to barriers to entry or expansion, as well as how to restore competition where such barriers are found to exist in ways that comply with data protection rules; (ii) assessing competition on privacy quality as this is understood by consumers, particularly in light of corporate practices that aim to maximise the collection of consumer data by influencing consumer behaviour and that may hinder such competition; and (iii) evaluating claims that the implementation of data protection standards by dominant digital gatekeepers harms competition by restricting customers' or rivals' access to data.

3.2.1. Barriers to entry or expansion

45. Various reports and market studies by competition authorities and other observers have described factors that make it difficult to dislodge incumbents in many digital markets in which data plays an important role. The Special Advisers to Commissioner Margrethe Vestager emphasised extreme returns to scale, the prominence of network externalities and the role of data in creating strong economies of scope that favour the development of large ecosystems and give the incumbents controlling them a significant competitive advantage.[43] Large platforms with many users and diverse product offerings are uniquely placed to gather first-party datasets, rich both in the number of users and the data points available for each user.[44]

46. The richness of this data is further enhanced by the extensive third party data gathered by certain platforms via the use of cookies, pixels, user log-in capabilities and other methods by which companies such as Facebook and Google track users even when

[41] See, e.g., the concept of 'privacy policy tying' according to which a platform dominant in an 'origin market' can enter and monopolise a target market by gaining user consent to combine data from both markets, thereby allowing the platform to fund services in the target market from the monetisation of data in the origin market where it is dominant. D. Condorelli & J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", 14 December 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504025.

[42] DAF/COMP(2020)1, Consumer Data Rights and Competition – Background Note by the Secretariat, pages 32-40.

[43] See Crémer, de Montjoye & Schweitzer, supra note 19, Executive Summary, pages 2-3.

[44] For a discussion on the value of rich and diverse datasets, see e.g. Stigler Center for the Study of the Economy and the State (2019). *Stigler Committee on Digital Platforms - Final Report*, pp.44-51. Available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf, accessed on 4 May 2020.

they are on other websites. The ease of collecting data on consumer behaviour (without prejudice to whether the collection is done in compliance with the GDPR), combined with the fact that many digital markets have tipped towards one or two incumbents has led to a situation in which, as noted in one study, "… *a few "gatekeeper" firms are in a position to control the tracking and linking of those behaviours across platforms, online services, and sites – for billions of users. As a result, chronicles of peoples' actions, desires, interests, and mere intentions are collected by third parties, often without individuals' knowledge […], with a scope, breadth, and detail that are arguably without precedent in human history*."[45]

47. The Australian Competition and Consumer Commission's Digital Platforms Inquiry concluded that "[*t]he breadth and depth of user data collected by the incumbent digital platforms provides them with a strong competitive advantage, creating barriers to rivals entering and expanding in relevant markets, and allowing the incumbent digital platforms to expand into adjacent markets*."[46]

48. The academic literature is divided on the extent to which data itself can be a driver of competitive advantage. Some commentators broadly agree with the above, whereas others claim that additional data eventually starts to yield declining marginal returns and that factors such as engineering talent are more important for consistent success. Nevertheless, there is broad agreement that 'data' is heterogeneous and that any analysis of whether a specific set of data held by an incumbent creates or strengthens a competitive advantage must be performed on a case-by-case basis, with a view to determining whether access to the dataset is unique or replicable.

49. The UK Competition and Markets Authority's (CMA's) interim report in its market study on digital platforms and online advertising detailed its preliminary findings on the role of data in relation to the market power held by Facebook in social networks and social network advertising, and Google in relation to search, search advertising and open display advertising. The CMA's preliminary findings were that data gives platforms a competitive advantage in the provision of both consumer-facing and advertising services. Google's superior access to a greater volume of click-and-query search data enables it to deliver more relevant results. In digital advertising, platforms provide targeting capabilities allowing advertisers to target current and potential customers and reach wider audiences. Advertisers choose platforms with detailed data on users. Google and Facebook have a competitive advantage in advertising because they collect a large amount and variety of data types from their consumer-facing services and their broad coverage of third-party sites and apps. This sets them apart from rival platforms such as Microsoft and Amazon in relation to the ability to monetise consumer data through advertising.[47]

50. If it is accepted that access to data can create a competitive advantage for incumbents, and that the competitiveness of firms in certain markets will depend on timely access to relevant data and the ability to use it to develop new and innovative products, access obligations arising from sector-specific regulation, or competition enforcement (if the data is held by firms with market power engaging in exclusionary conduct), may be envisioned. In the latter context, the essential facilities doctrine has been proposed as a model that could be adapted and applied in certain cases to obligate dominant undertakings to give rivals access to specific data, if it can be established that the data itself is

[45] Acquisti, Taylor & Wagman (2016), "The Economics of Privacy", Journal of Economic Literature, Volume 54/2, pp. 442-492.

[46] ACCC Digital Platforms Inquiry, supra note 8, page 2.

[47] CMA interim report, supra note 8, Appendix E 'The role of data.'

indispensable to compete, and provided the remedy can be implemented in compliance with the data protection rules. A full discussion of the essential facilities doctrine and its application to digital markets generally is outside the scope of this contribution, but questions have been raised in relation to how to apply the underlying rationale of that doctrine to data, as well as the privacy considerations inherent in the concept of giving third parties access to consumer data. Suffice to say here that it might not be possible (or even appropriate) to adopt a one-size-fits-all approach in light of the various types of data and the different contexts in which a request for access to data might take place. No appropriate test case has yet arisen, although authorities are likely to encounter such cases in the future.

3.2.2. Assessing competition on privacy

51. Part 1 of this paper outlined recent survey results in the EU showing that significant proportions of consumers are generally interested in how businesses collect and use their personal data. Market investigations in specific cases, such as *Microsoft/LinkedIn*, have further supported the view that data protection standards can be an important parameter of competition, particularly in markets characterised by zero-price platform services where the undertaking has an incentive to collect as much data as possible in order to better monetise it on the other side of the platform.

52. However, the appreciation of consumer attitudes towards privacy in the context of competition assessments remains complicated by the sheer scale and complexity of data collection practices engaged in by economic operators, including the largest digital platforms. Moreover, businesses may also engage in 'concealed data practices' that offer weak protection to consumers in relation to their data but hide the true extent of the data collection and use by means of vague descriptions and complicated policy structures. It has been argued that such practices, which may be in breach of the GDPR and are subject to ongoing enforcement actions by DPAs, may also impose harms on consumers that competition authorities should take into account.[48]

53. Concerns have also been raised about the 'take-it-or-leave-it' nature of privacy terms and conditions, particularly in respect of markets characterised by an apparent lack of competition. Indeed, such notices were at the heart of the Bundeskartellamt's case against Facebook, brought under German law The prevalence of such notices evidences a lack of bargaining power held by consumers, suggesting that consumers may care about privacy in a general way but may, in a sense, resign themselves to inadequate safeguards offered by powerful incumbents due to a lack of alternatives.

54. These considerations also imply that competition, both on privacy standards and for the development of innovative privacy-enhancing services and technologies, in part depends on the ability of consumers to effectively select and enforce preferences for greater privacy protection.

55. Incentives for undertakings to compete on privacy and provide effective means of data portability will be enhanced to the degree that consumers understand how their data is being used and for what purposes. The GDPR contributes to stimulating such competition by incorporating the principles of data protection by design and by default, which create incentives for innovative solutions that take data protection considerations from the outset.[49] Likewise, by preventing lock-in to incumbents, an effective right to data

[48] See K. Kemp, "Concealed Data Practices and Competition Law: Why Privacy Matters", UNSW Law Research Paper No. 19-53 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769.

[49] GDPR, Article 25.

portability exercised by informed consumers serves to lower barriers to entry for smaller operators offering innovative services.

56. In the EU, questions related to the clarity and legibility of privacy information and the validity of consent for the processing of personal data are specifically covered by the GDPR and enforced by the DPAs of the Member States. In this regard, the effects of a number of forthcoming enforcement decisions by the DPAs may significantly affect the use of certain data practices, including by the large platforms. Consumer protection law may also have an important role to play due to its specific focus on addressing asymmetries of information and ensuring that consumers are not deceived or misled. Although competition law enforcement may not be the most appropriate forum for addressing these concerns as such, competition authorities seeking to evaluate competition on privacy as an element of quality in specific cases should observe developments in data protection enforcement that affect the practices of undertakings and be aware of factors which can influence effective consumer-led enforcement of privacy preferences and incentives for businesses to offer consumers strong privacy protection.

3.2.3. Privacy-based justifications in the context of access to data

57. Market participants in various contexts and jurisdictions have raised concerns that large platforms such as Google and Facebook may invoke the privacy interests of consumers as justifications for policy changes that restrict the sharing of important data with third parties, thereby consolidating their own market position. A related development is the increasing trend of browsers banning third-party cookies, limiting the ability of smaller publishers and rivals of platforms such as Google (with a strong position in both browsers and various advertising services) to collect sufficient data to engage in effective targeting and measure the effectiveness of their services.

58. The details of these concerns are complex and still preliminary, and may involve misconceptions about what data protection rules require. Where such misconceptions would be relevant, guidance and enforcement actions by privacy regulators can contribute to clarify the lawfulness of certain practices. At the same time, in light of the importance of personal data to the online advertising sector and the prominence of undertakings such as Google and Facebook in these markets, competition authorities may eventually be faced with the task of investigating the competitive effects of conduct involving personal data access restrictions imposed by undertakings citing privacy concerns as justification. Further fact-finding is needed to begin building a coherent analytical framework, in addition to the further exploration of modalities of effective cooperation between competition and data protection authorities.