**The Dickson Poon**

**School of Law**

**Writing Project Cover Sheet – 2018/19**

**(Dissertation)**

| | |
|---|---|
| Dissertation Module Code: | 7FFLX001 |
| Module Title: | LLM Dissertation, 40 Credit |
| Candidate Number: | Z18049 |
| LLM Pathway/Specialism: | LLM in Competition Law |
| Dissertation Supervisor: | Professor Alison Jones |
| Dissertation Title: | Fostering Competition in Online Platforms through Mandatory Data Sharing and the Implications for Data Protection |
| Submission Date: | 2 September 2019 |
| Word Count: | 2998 |

## INTRODUCTION

The digital economy has always been characterised by the collection and the analysis of data. Yet, recent technologies have substantially changed the dynamics of data-driven markets and increased the value of data.[1] Information is now collected much quicker and in much greater quantities, which has given rise to the term 'Big Data'.[2]

As such, the detention of data is not problematic. But, in some circumstances, controlling large datasets constitutes a significant competitive advantage. This can be observed in the context of online platforms where markets often tip towards the establishment of dominant firms being close to monopolies. The increasing role of data in digital markets comes together with various discussions on the difficulties for new entrants to enter markets and compete with current incumbents. It is desirable for competition authorities to tackle these new issues arising from access to data. One way to do so is trough Article 102 TFEU. However, intervention through competition law is not always the most appropriate solution. This paper therefore argues that regulation would be a more appropriate means to deal with data access issues.

## MANDATORY DATA SHARING THROUGH REGULATION

### Rationale for establishing a regulatory regime

Article 102 TFEU only enables competition authorities to intervene *ex post*, to sanction abuses. However, *ex post* intervention prevents businesses holding large amount of data from having legal certainty as to when and with whom they should share data. Moreover, competition proceedings can be considerably long. In the context of refusals to deal cases, *Magill* proceedings lasted for 10 years while *Microsoft* proceedings lasted for more than 14

[1] EDPS Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data (2018) <available at https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf> 6.
[2] B Lasserre and A Mundt, 'Competition Law and Big Data: The Enforcers' View' (2017) 1 Italian Antitrust Review 87.

years.[3] Furthermore, Article 102 only applies to dominant firms. Dominance might not only be difficult to prove in the context of data but one might also encounter scenarios where a firm is not dominant and where data sharing might still be desirable. Finally, competition agencies are perhaps not the best placed to determine the modalities of data sharing such as the price, the type and quantity of data to be shared. Neither do they have the tools to monitor compliance with such a remedy.[4]

Regulation might therefore have a role to play in improving competition in digital markets and in avoiding that incumbents manage to control the whole online environment. Mandatory data sharing might indeed be an option to foster competition by enabling competitors to access data and thus enter digital markets more easily. Prüfer and Schottmuller show that in markets characterised by strong indirect network effects, a regulatory intervention would lead to more innovation and higher consumer welfare. In fact, encouraging more competition in online platforms is likely to incentivise both the incumbents and new competitors to innovate.[5]

**Limits of data portability as an alternative to mandatory data sharing**

Data portability provided for in Article 20 of the GDPR[6] is a first step in terms of exchanges of data between undertakings. It enables users of a digital service to request access to their personal data from a particular data controller and transfer it to another.

Data portability set out in the GDPR and competition law may complement each other. On the one hand, data portability can go further than competition law and foster competition where the conditions for an abusive refusal to deal are not met. On the other hand, competition law could broaden the scope of data portability by taking into consideration the interests of

[3] In that sense see J Drexl and others, 'Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition on the Current European Debate' (2016) available at <https://ssrn.com/abstract=2833165> ; Spindler (n 18) 404.
[4] V Kathuria and J Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy - Max Planck Institute for Innovation and Competition Research Paper' (2019) available at < https://ssrn.com/abstract=3337524> 16.
[5] J Prüfer and C Schottmuller, 'Competing with Big Data' (2017) 6 TILEC Discussion Paper 6 ; I Graef and J Prüfer, 'Mandated data sharing is a necessity in specific sector' (2018) Economisch Statistische Berichten 300.
[6] Regulation No 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 85/46 (General Data Protection Regulation) [2016] OJ L119/1.

companies in addition to those of individuals and, for instance, provide access to non-personal data.[7]

Data portability favours competition by enabling competitors to acquire access to personal datasets. However, various arguments show that data portability cannot adequately tackle competition issues in digital markets. First, consumers are not sufficiently aware of the positive effects engendered by the transfer of their data, namely the achievement of higher quality in the services provided to them. Hence, there might not be enough switching so as to enable potential competitors to effectively compete with the dominants.[8] Secondly, data portability only relates to information provided by the data subject. This means that data that was inferred or derived by data controllers fall outside of Article 20 of the GDPR.[9] Thirdly, data portability necessitates the consent of the data subjects. It is likely that data subjects will not exercise their right in favour of small firms, willing to enter the market, as there is at that early stage no guarantee of their success that might incentivise consumers to transfer their data to them. Finally and most importantly, data portability is a right conferred to consumers who will exercise it following their own personal interests. On the contrary, competition authorities intervene to protect the general interest and are therefore much better placed to preserve competition.

Data portability thus constitutes an important step in the path towards data sharing. However, it might not always provide adequate solutions. And given that competition law remedies are not always appropriate either, it might be necessary to adopt a distinct specific regulation on data sharing.

**Specific regime for data sharing**

Establishing a specific regime for data sharing is a complex task. It requires reflecting on different issues such as, for instance, the person to whom data should be transferred, the period during which data should be shared, the format of data and the conditions imposed on

[7] A Diker Vanberg and MB Ünver, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' (2017) 8 European Journal of Law and Technology 12.
[8] Graef and Prüfer (n 5) 300.
[9] O Lynskey, 'Aligning data protection with competiton law remedies' (2017) European Law Review 799.

the firms receiving the data. [10]

On this question, Mayer-Schöneberger and Ramge made an interesting proposal, based on what they call a 'progressive data sharing mandate'. They suggest that data sharing should be mandated in situations where a firm has more than ten percent of market share for instance. In such a case, the firm would have to share a part of its data with whoever requests access to it. Moreover, the more market power the firm has, the more data it will have to share with third parties. [11]

To build up such a regime, one could also take inspiration from legislative initiatives undertaken in other sectors.[12] For instance, one could have regard to the Second Payment Services Directive (PSD2).[13] These rules were adopted to enhance competition in the banking sector. They enable Fintech companies to have access to bank account's information when this is necessary to offer new services to bank accounts' holders, but only for the purposes required by the customer.[14]

Some argue that exclusive access to data should be the exception while the exchange of data should be the new basic rule.[15] However, as suggested by Schepp and Wambach, mandating access through regulation should only be undertaken in specific circumstances, namely where significant barriers prevent competitors to enter the market.[16] This is important as especially for smaller players, having to share data implies costs, which might make it more difficult to recover their initial investments. Small firms might thus be deterred to enter markets when compliance with the obligations to share data is too burdensome.[17]

It would also be necessary to technically ensure that the data that is exchanged can be processed by the company receiving it. One possibility would be to impose standardisation of

[10] D Tucker and H Wellford, 'Big Mistakes Regarding Big Data' (2014) 14 Antitrust Source 11.
[11] V Mayer-Schöneberger and T Ramge, *Reinventing Capitalism in the Age of Big Data* (John Murray Publishers 2018) 167.
[12] Commission Staff Working Document of 10 January 2017 on the free flow of data and emerging issues of the European data economy 21, SWD(2017) 2 final.
[13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market [2015] OJ L337/35.
[14] S Vezzoso, 'Fintech, Access to Data, and the Role of Competition Policy' (2018) available at <https://ssrn.com/abstract=3106594> 32.
[15] M Camps, 'Maintaining focus amid blurring boundaries' (2018) Economisch Statistische Berichten 8.
[16] N-P Schepp and A Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (2016) Journal of European Competition Law & Practice 120.
[17] I Graef, S Wahyuningtyas and P Valcke, 'Assessing data access issues in online platforms' (2015) 39 Telecommunications Policy 9.

data formats.[18] Some authors point out that standardisation hinders technological innovation when an industry is stuck with an 'inefficient standard'.[19] But standards can and should evolve and one might also want to find options to incentivise firms to cooperate in order to maintain standards at the highest level of technology. Moreover, in order to reduce costs for small players and new entrants, one might want to limit mandatory standardisation only to powerful companies that detain a certain amount of data.[20]

One has to acknowledge that many uncertainties remain. This does not mean however that the option should be abandoned. On the contrary, competition authorities should work closely together and increase their efforts to find solutions.

## IMPLICATIONS OF DATA SHARING FOR THE RIGHT TO DATA PROTECTION

When reflecting on mandatory data sharing, one should not forget that data is distinct from other facilities. A significant quantity of data that is collected nowadays relates to identifiable or identified natural persons and thus qualifies as personal data.[21]

### Violation of the GDPR as a result of forced data sharing?

#### *Conditions for lawful sharing*

At the outset, it should be noted that the term personal data is interpreted broadly. According to the ECJ, any information which enables a company to identify a data subject with the help of additional data constitutes personal data.[22] The GDPR imposes different obligations upon firms processing personal data, also called 'data controllers'. Data sharing equates to making data available and thus amounts to data processing under Article 4(2) of the GDPR.

[18] S Louven, ' Shaping competition policy in the era of digitization – Access to Data' (2018) available at <http://ec.europa.eu/competition/information/digitisation_2018/contributions/sebastian_louven_oldenburg_centre_for_law_of_the_information_society.pdf> 7.
[19] M Gal and D Rubinfeld, 'Data Standardization' (2019) available at <https://ssrn.com/abstract=3326377> 15 ; H Richter and P Slowinski, 'The Data Sharing Economy: On the Emergence of New Intermediaries' (2018) 50 IIC 19.
[20] M Gal and D Rubinfeld (n 19) 28.
[21] For instance, information such as IP addresses generally qualifies as personal data.
[22] Case C-582/14, *Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para 49.

Personal data may be processed only in specific circumstances set out in Article 6 of the GDPR. For instance, data can be processed where the data subject has consented to it and where the processing is necessary to comply with legal obligations.[23] The processing of personal data must also be transparent, serve 'specified, explicit and legitimate purposes' and not go beyond what is necessary to achieve these purposes.[24]

***Mandatory data sharing as a competition law remedy***

Some argue that a decision mandating access to data by a competition authority could constitute a legitimate ground for the transmission of data. For instance, according to Graef, the decision could amount to a legal obligation and data could thus be processed legally under Article 6(1)(c) of the GDPR.[25] More specifically, the legal obligation would derive from Article 102 TFEU and from the related case law of the ECJ. If the other conditions of the GDPR are fulfilled, data sharing ordered by a competition authority would therefore not amount to a violation of the GDPR.

However, there is no certainty the relevant courts and agencies would accept such a broad interpretation of the GDPR. As demonstrated by some authors, the term legal obligation should not be understood as a general legal rule such as Article 102 TFEU but rather as a clear and detailed legal basis setting out the modalities of data procession.[26] In any case, even though this legal ground could be admissible in theory, as a matter of coherence of EU law, competition authorities should refrain themselves from adopting such decisions without ensuring that the right to privacy is preserved. Indeed, even if there might not be a formal violation of the GDPR, such an outcome would be problematic in the light of its objectives, namely the protection of personal data.

**Possible reconciliation between data sharing and data protection rules**

[23] GDPR, Article 6(a) and 6(c).
[24] GDPR, Article 1(a)(b)(c).
[25] I Graef, 'Naar een meer samenhangend mededingings- en gegevensbeschermings- toezicht in datagedreven markten' (2018) Tijdschrift voor Toezicht 40.
[26] V Kathuria and J Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limiations of Data Sharing Remedy - Max Planck Institute for Innovation and Competition Research Paper' (2019) available at < https://ssrn.com/abstract=3337524> 22.

In view of the risks of GDPR violations, competition authorities – when imposing remedies – but also regulators – when contemplating the adoption of a new data sharing regulation – should aim at finding a balance between enhancing competition and at the same time preserving the right to data protection.

***Obtaining the consent of data subjects***

One possible legal ground that could be used in the context of mandatory data sharing is the consent of data subjects. Under Article 6(a) of the GDPR, data subjects must agree before their data is shared with third parties and receive precise information as with whom and for what purpose their data will be shared. This probably implies that consent for the sharing of data should be obtained by the dominant firm required to share data with its competitors. But companies receiving personal data as a result of mandatory data sharing should in turn inform data subjects on what they will use their data for.[27]

In that sense, the French Autorité de la concurrence required GDF Suez to give access to personal data it had previously collected to some of its competitors. For that purpose, it established an opt-out system whereby customers had to express their refusal in order to prevent the transfer of their personal information to competing gas providers.[28] Such a solution would probably not comply with the GDPR. The latter instrument is very strict in assessing consent and an opt-out system would not meet the threshold necessary for consent to be informed and completely unambiguous. This is because consent cannot be inferred from the absence of reaction from individuals and requires a positive action from the subjects.[29]

Besides, the condition of consent should not be envisaged on its own. Data subjects have other rights under the GDPR. Among others, they have a right to access, rectify and erase their personal information but also to withdraw their consent and to receive explanations. Hence, even where firms have received initial consent from consumers to share their data, the

[27] GDPR, Articles 13 and 14 ; G Colangelo and M Maggiolino, 'Data access and AI: Antitrust vs Regulation' (2018), available at <http://ec.europa.eu/competition/information/digitisation_2018/contributions/giuseppe_colangelo_mariateresa_maggiolino.pdf> 6.

[28] Autorité de la concurrence, Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentées par la société Direct Energie, available at <http://www.autoritedelaconcurrence.fr/pdf/avis/%2014mc02.pdf.>, paras 169-174 ; I Graef, 'Naar een meer samenhangend mededingings- en gegevensbeschermings- toezicht in datagedreven markten' (2018) Tijdschrift voor Toezicht 40.

[29] GDPR, Recital 32.

latter might find it significantly complex to exercise their rights when their data circulates amongst many companies.[30] They might not be able to identify the firm they should address their requests to and their right to data protection might thus be weakened. This is why it is more desirable and practical to opt for other solutions such as the anonymisation of personal data.

***Pseudonymised and anonymised data***

Pseudonymisation is understood as a way of processing personal data after which the data processed can no longer be linked to an individual without using some additional information.[31] Encryption can be more or less secured but it might lead the entity detaining the key to trace back the identity of the person whose data was encrypted. Hence, pseudonymisation is not sufficient to guarantee the protection of personal data as it can still lead to the identification of a natural person.[32]

Anonymisation could potentially solve the issue of data protection. For instance, it would be possible to anonymise data related to the click tendencies of users following their search queries.[33] To fall outside of the scope of data protection rules, anonymisation needs to be irreversible in the sense that the data can no longer be linked to a natural person.[34] However, the development of new technologies makes re-identification of individuals easier so that perfect anonymisation is difficult to guarantee and will surely become more complex in the future.[35] It has even been demonstrated that de-anonymisation of data can be operated relatively easily by computer scientists.[36]

Despite these difficulties, anonymisation of data in the context of mandatory data sharing seems to be one of the most feasible options. But to guarantee that anonymisation is effective, one should calculate the risks of re-identification in each specific case. Then, the greater these

[30] G Colangelo and M Maggiolino, 'Data access and AI: Antitrust vs Regulation' (2018), available at <http://ec.europa.eu/competition/information/digitisation_2018/contributions/giuseppe_colangelo_mariateresa_maggiolino.pdf> 6.
[31] GDPR, Article 4(5).
[32] GDPR, Recital 26.
[33] M Camps (n 15) 8.
[34] Article 29 Working Party 'Opinion 05/2014 on Anonymisation Techniques' (2014) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[35] Graef and Prüfer (n 5) 300.
[36] P Ohm, 'Broken Promises of Privacy: Responding to the surprising failure of anonymization' (2010) 57 UCLA Law Review 1716.

risks, the more cautious one should be in choosing and monitoring the anonymisation technique. Data access remedies or regulation should therefore be tailored by taking into account the characteristics of specific sectors so as to ensure that the data shared could in no way be linked to an identifiable natural person.[37] According to the GDPR, the re-identification of data subjects must be impossible for the person receiving the access.[38] Powerful online platforms are more likely to be able to de-anonymise data and should therefore be subject to a stricter monitoring when they access anonymised information.

Broadly speaking, anonymisation can be operated via two techniques: randomisation and generalisation. Randomisation aims at suppressing the link between the data subject and the information. This can be done for instance through noise addition which alters data to make it less accurate but without modifying it too much and make it completely useless. Permutation of data is also a form of randomisation and consists of moving information around so that data related to one individual can no longer be linked together in order to identify that individual.[39] Generalisation is a technique which generalises or dilutes personal information through the alteration of the scale, the magnitude or the precision of data.[40] Aggregation of data is an example of generalisation and regroups large amounts of data together. Different techniques may also be combined to prevent the de-anonymisation of data.[41] For instance, one could combine noise addition, permutation, and aggregation of data.[42] The more measures are taken, the stronger the anonymisation will be and the better the data will be protected. In the same vein, experts appointed by the Commission also suggest using security mechanisms such as 'remote access' systems as well as 'question-and-answer' systems. These techniques make data access possible not through exchanging copies of datasets but through granting access to virtual systems that enable data analysts to use the available datasets but within certain limits and controls.[43]

---

[37] G Zanfir 'The right to Data portability in the context of the EU data protection reform' (2012) 2 International Data Privacy Law 155.
[38] J Crémer, Y-A de Montjoye and H Schweitzer, 'Competition policy for the digital era' (2019) available at < http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> 76.
[39] Data Protection Commission, 'Guidance on Anonymisation and Pseudonymisation' (2019) available at <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf> 11.
[40] Article 29 Working Party (n 34) 16.
[41] V Kathuria and J Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limiations of Data Sharing Remedy - Max Planck Institute for Innovation and Competition Research Paper' (2019) available at < https://ssrn.com/abstract=3337524> 31.
[42] Article 29 Working Party (n 34) 9.
[43] Crémer, de Montjoye and Schweitzer (n 38) 86.

Unfortunately, besides these legal concepts, there is almost no guidance as to the way and the circumstances in which the techniques should be used to anonymise data. It will thus be essential to further research on the matter in order to determine what can be considered as the most secured option. For now, the method of anonymisation should be assessed on a case-by-case basis, depending on the risks of re-identification as a specific method might be more effective in one case while it will not be appropriate in another.

***Cooperation between the relevant authorities***

In any case, when contemplating competition remedies or a specific regime for data sharing, data protection authorities should be involved in the discussions. This is essential to preserve the coherence of the EU legal order. Competition law cannot be envisaged on its own, independently of other areas of EU law. When competition enforcement leads to data protection issues, competition authorities should take these into account. In such cases, the relevant data protection authorities should play a role that goes beyond giving advices.[44] When data sharing is made compulsory through competition enforcement, experts in data protection – both at the EU and at the national level – should be able to oppose such a remedy where it does not guarantee a sufficient level of data protection for data subjects concerned by the sharing.

## CONCLUSION

The digital sector is uncertain but it is now urgent to seek ways to neutralise platforms giants' market power. Data access remedies may fulfil this role and foster competition online. However, these remedies cannot be implemented without ensuring that users' personal data is effectively protected. Preserving competition law and data protection law are two fundamental policies in the EU and one should not favour one over the other. It is necessary to find ways to implement data access remedies while not interfering with data protection laws. To that end, guidance should be given on how to anonymise data so as to ensure a highly secured protection of users' personal data.

[44] I Graef, *EU Competition Law, Data Protection and Online Platforms – Data as Essential Facility* (Wolters Kluwer 2016) 320.