The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?

Aysem Diker Vanberg [1] and Mehmet Bilal Ünver [2] [3]

Cite as Diker Vanberg, A. & , Ünver, MB., "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", in European Journal of Law and Technology, Vol 8, No 1, 2017.

ABSTRACT

The EU General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union on 4 May 2016 [4] . It will become applicable on May 25, 2018. The GDPR comprises a new right to data portability for individuals, which requires data controllers to ensure that they can hand over the personal data that has been provided by the data subject himself/herself, in a structured, commonly used and transferable format.

This paper critically examines the right to data portability and suggests that in order to ensure comprehensive data portability that reaches out to all relevant stakeholders, including businesses, the provisions in the GDPR need to be analysed by taking into account EU competition rules. It suggests that lessons can be drawn from EU competition law to limit the potential adverse consequences of the right to data portability particularly for small and medium-sized enterprises. It also asserts that EU competition rules, especially Article 102 TFEU and the essential facilities doctrine, can complement data portability by facilitating mandatory access to specific data.

Keywords: The General Data Protection Regulation; article 20 of the GDPR; article 102 TFEU; data; data controller; the right to data portability; API; controller to controller transfer; competition law; essential facilities doctrine; network effects; Data Protection Directive

1. INTRODUCTION

On 25 January 2012, the Commission proposed a reform of the EU's data protection rules by drafting the General Data Protection Regulation (GDPR) in order to strengthen online data protection rights and boost Europe's digital economy. It was also done to adapt to technological advancements that had taken place in the previous decade, following the introduction of the Data Protection Directive [5] . The reactions to the GDPR have been mixed. Some scholars [6] saw it as a welcome development, however while others [7] have raised concerns.

The right to data portability in the GDPR will require businesses to ensure that they can hand over the personal data provided by an individual himself/herself in a usable and transferable format [8] . The preamble of the GDPR demonstrates that the right to data portability is not just limited to social networking sites but will also be applicable to cloud computing, web services, smartphone systems and other automated data processing systems [9] . The right to data portability will apply to a wide range of areas such as social media, search engines, photo storage, email or online shops. It will be equally applicable to banks, pharmaceutical companies, energy providers, airlines - even small businesses like pizza shops or tailors if they are data controllers.

The final text of the GDPR was agreed in the trilogue between the Council, Parliament and the European Commission on 15 December 2015, and published on 4 May 2016 in the Official Journal of the European Union [10] . After a two-year transition period, the GDPR will be binding on all member states from 25 May 2018.

The right to data portability is contained under Article 20 of the GDPR. It can be seen as an extension of an individual's right of access under Article 15 of the GDPR [11] . It has two key elements: the right of the data subject to obtain a copy of personal data from the data controller and the right to transfer that data from one data controller to another. The text limits the scope of the right to data portability to a great extent by adding that the controller would only transfer the data to another controller, where such a transfer is 'technically feasible'. As explained below this is quite problematic as the GDPR provides no explanation as to what is meant by technically feasible, which might give significant leeway to data controllers who may wish to not transfer the data to another data controller. Furthermore, another limitation of the right to data portability, is that it only applies to personal data provided by the data subject him/herself.

Article 20 of the GDPR addresses the issue of data portability specifically from the perspective of the individual users and is not concerned with the rights of businesses, in particular other service providers and competitors. Arguably, due to the importance of data portability not only for individual users but for all stakeholders concerned particularly for businesses, the provision in this form is not sufficient to ensure data portability across the board and needs to be supplemented by existing EU competition law provisions.

This paper critically examines the right to data portability under the GDPR to establish whether EU competition law can be useful to complement the gaps in the GDPR. It also examines whether there are lessons to be drawn from EU competition law. The paper is divided into five sections. Section 2 critically analyses the issues raised by Article 20 of the GDPR and potential enforcement problems. Section 3 discusses the application and suitability of EU competition rules, particularly the essential facilities doctrine in the data portability

context. Section 4 analyses key cases pertaining to data portability and the use of personal data. Finally in Section 5, conclusions are drawn as to the future of the right to data portability.

2. CRITICAL REVIEW OF THE RIGHT TO DATA PORTABILITY

2.1 KEY ISSUES IN THE GDPR

2.1.1 LIMITATIONS ON DATA GENERATED BY THE DATA CONTROLLER

Article 20 of the GDPR only applies to data provided by the data subject himself/herself. The Article 29 Working Party published a summary of the discussions that took place on July 26, 2016, at the Fablab Workshop [12] . It gives a good overview of the key issues in relation to data portability. As pointed out in this document, the interpretation of data that has been provided by the data subject himself/herself requires clarification, as a narrow interpretation of this would result in fewer benefits for individuals whilst a wide interpretation of this concept would be a concern for data controllers [13] .

As mentioned by Graef et al, despite the lack of clarity, Article 20 of the GDPR will potentially not cover the transfer of data that has been generated by the service provider for statistical and analytical purposes such as online reputations [14] .

As Graef et al point out, [15] in an auction website like eBay the contact information and the advertisements are provided by the seller (data subject) himself but the provider adds feedback scores to the seller's profile and these form part of the reputation that a seller has built on. Hence, a literal interpretation of the adopted text would only allow the users to move their personal information to another auction site whilst not being able to move their ratings and reputation to another auction site as the latter is provided by the service provider. For an online user it is crucial to show that he/she has built a good reputation when he/she moves on to a different platform. Without moving this reputation, it is highly unlikely that the seller would attract new buyers in a new platform. Ultimately, this might hinder users from moving to another platform.

In the light of above it might be argued that the wording of the Article 20 of the GDPR limits the scope of the right to data portability to a great extent.

2.1.2 PRIVACY RIGHTS OF THIRD PARTIES

Another limitation of the right to data portability concerns the privacy rights of third parties. If the data requested by the data subject concerns information pertaining to other individuals, then such a request can be denied by the data controller as it might adversely affect the rights and freedoms of others. As noted by Engels, allowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user [16] . For example, when several people appear in a photograph on Facebook, even if one data subject wants to import it to another social networking platform, this cannot be done, as it would impact privacy and data portability rights of other individuals appearing in that picture. This implication seems to have been taken into account by the legislators as paragraph 4 of Article 20 GDPR states that the right to data shall not adversely affect the rights and freedoms of others'. This delimitation is likely to discourage users from invoking Article 20 of the GDPR.

2.1.3 TECHNICAL FEASIBILITY OF DATA TRANSFER

As mentioned above, another challenge for the enforcement of the right to data portability concerns the 'technical feasibility' sought for the data portability across the platforms. Arguably, what is technically feasible for one data controller might not be technically feasible for another data controller. Given the wording of Article 20(2) of the GDPR it is likely that some data controllers will contend that such a transfer is technically infeasible. As a result of this wording the transfer of data may be undermined and overlooked by data controllers. As there is no reference to the Commission's authority to specify the electronic format necessary for data portability in the GDPR, collaboration among market players is crucial in devising industry norms and standards.

2.1.4 DISPROPORTIONATE COSTS AND EFFORTS

Forcing data controllers to transfer personal data may incur disproportionate costs and efforts.

Article 20 of the GDPR requires an online service to write specialised code (export-import module, (EIM)) that will export data from that service and import it to another service. As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider [17] .

Neither the Commission nor other EU institutions have presented any figures as to the cost of complying with data portability requests. According to a study by Christensen et al, the GDPR reform would increase European small and medium-sized enterprises' annual IT costs by between approximately € 3.000 and € 7.200 depending on the industry the particular SME is operating in, representing between 16 and 40 per cent of their yearly average IT budgets [18] . It is not clear what percentage of this budget will be spent responding to data portability requests.

Swire and Lagos also support this point and argue that the GDPR would impose substantial costs on suppliers of software and apps [19] .

Whilst such costs may not be significant for large companies, the requirement is likely to create problems for small and medium-sized companies. It must be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 per cent of the total worldwide annual turnover of the preceding year, whichever is greater.

The issue of disproportionate costs was also raised in December 2015 by Baroness Neville Rolfe, the UK's parliamentary Under-Secretary of State for the Department for Business, Innovation and Skills. She stated that data portability rules designed to enable consumers to move their data from one platform to another should not be too costly as they can serve as an entry barrier into markets, and this might have an adverse effect on innovation and competition [20] .

2.1.5 TRANSFER OF DATA MAY COMPROMISE VALUABLE PROPRIETARY INFORMATION AND INTELLECTUAL PROPERTY

If the personal data that needs to be transferred comprise valuable proprietary information and intellectual property, this might discourage companies/service providers from creating the proprietary information in the first place.

The case of True Fit [21] , an online digital service helping users of online clothing retailers such as House of Fraser to find the right cloth sizes for their shoppers, illustrates this point. The True Fit service asks shoppers to share a wide range of personal data such as height, weight, measurements, body type - and information like what brand and size their favourite clothing come from. Users share this information with True Fit, which then shares it with online retailers. If True Fit were to be required under the data portability provision to transfer this data to other retailers, its business model would become obsolete.

Recital 63 of the GDPR provides that the general right of access under Article 15 could be restricted if it adversely affects the rights and freedoms of others, including trade secrets and intellectual property rights. As the right to data portability can be seen as an extension of the right of access, arguably the limitation mentioned in Recital 63 should be applicable in the context of data portability requests. In other words, when faced with data portability requests companies, should be able to strip valuable data from the dataset if it adversely affects trade secrets and intellectual property.

Nevertheless neither recital 68 of the GDPR pertaining to the limitations of the right to data portability, nor Article 20 of the GDPR specifically suggests that the right to data portability can be limited if it is adversely affects trade secrets and intellectual property. Hence there is a need for further clarification as to whether the right to data portability might be restricted when it affects proprietary information and intellectual property rights.

If companies like True Fit stop creating valuable services based on personal data this will clearly have a stifling effect on competition and innovative solutions. This would ultimately have an adverse effect on consumers who would be deprived of choice and useful products.

2.1.6 ENFORCEMENT ISSUES PERTAINING TO THE RIGHT TO DATA PORTABILITY

As noted by the Article 29 Working Party, there is a need for guidance on how the right to data portability is going to be enforced [22] .

The main objective of the right to data portability is to empower consumers so that they can get a copy of their electronic personal data, demand transmission of their personal data to another provider and switch to other providers [23] . Hence, the objective of the right to data portability overlaps with the objectives of other areas of law, e.g. competition law, consumer protection laws and so forth.

Similar to other data subject rights in the GDPR, data portability is a right, which needs to be invoked by the data subject and cannot be relied upon by parties such as small and medium sized businesses. For instance, a small business cannot demand data portability from its business bank but an individual can. This raises some problems regarding its legal and theoretical boundaries, as well as enforcement within the realm enshrined by the GDPR.

Furthermore, there is no clarity as to whether users will make use of the right to data portability. In order to ensure that the right is invoked effectively by data subjects, data subjects need to be informed as to what this right entails. Hence, Article 29 Working Party and particularly the national data protection agencies should have information on their websites in plain and simple language explaining users how they can approach the data controller for data portability requests and advise them how to make a complaint if the data controller refuses to provide the data. Making a complaint should be relatively easy and the data subjects should not incur substantial costs as this might discourage them from exercising their right.

2.1.7 PRIVACY AND DATA SECURITY RISKS

Security and privacy concerns arise when data is transferred from one data controller to another. Data can end up in the wrong hands if access is granted to the wrong person - an investigator making a pretext call, a conman engaged in identity theft, a hacker, or, in some instances, one family member in conflict with another [24] . Ironically, interoperable solutions as suggested in the GDPR [25] could aggravate security concerns at the expense of uniform rules and processes in this context. Although not seen as the main cause of the security vulnerabilities, interoperability is regarded as one of the factors that increases the number of opportunities for security breaches and the potential fall-out from such breaches [26] . Particularly for small and medium sized businesses (SME) with limited resources to invest in data security, this is a significant concern.

3. DATA PORTABILITY IN THE CONTEXT OF EU COMPETITION RULES

As noted by the former Commissioner for Competition Joaquin Almunia, data portability goes to the heart of competition policy as in a healthy competitive environment consumers can switch from one provider to another by taking their own data with them [27] . Data portability will indeed have a significant impact on avoiding consumer lock-in and switching costs. If switching from one service provider to another is too costly, the users of a service face a lock-in effect [28] . For instance, without data portability a consumer using Yahoo's email service might not want to move to Gmail due to the risk of losing invaluable personal data. This type of consumer lock-in could be seen as creating a more fragile marketplace, as it is open to exclusionary acts of dominant players. As such, the right to data portability needs to be considered also from a competition law viewpoint.

3.1 RELEVANCE AND APPLICABILITY OF EU COMPETITION RULES TO DATA PORTABILITY

Data controllers that refuse to move data to another controller can be subject to Article 102 Treaty on the Functioning of the European Union (TFEU) [29] investigations for the abuse of a dominant position.

Article 102 TFEU prohibits the abuse of a dominant position. The provision contains two key elements, namely the notion of dominance and the abuse of this dominant position. In order to apply Article 102 TFEU, firstly the undertaking in question needs to be in a dominant position in the relevant product market. The Court of Justice of the European Union (CJEU) defines dominance as a 'position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers

and ultimately of its consumers' [30] . In the past, the Commission and the European Courts relied on market share as evidence of a dominant position, particularly if it persisted over time. The Court of Justice stated the following in *Hoffman-La Roche* [31] *:*

> Although the importance of market shares may vary from one market to another the view may legitimately be taken that very large shares are in themselves, and save in exceptional circumstances, evidence of the existence of a dominant position. An undertaking which has a large market share and holds it for some time ... is by virtue of that share in a position of strength [32] .

As noted by the former Competition Commissioner Mario Monti, the Commission uses 'market definition and market shares as an easily available proxy for the measurement of market power enjoyed by the firms' [33] . As the Commission's Guidance Paper on Article 102 TFEU (hereinafter Guidance) [34] suggests, if the undertaking's market share is below 40 per cent, it is unlikely that the company would be held dominant in the relevant market. This demonstrates that undertakings with a market share of 40 and above are likely to be seen as a dominant undertaking by the European Commission. It must be noted that in technology intensive markets such as social networks, communication services, high market shares may not necessarily be indicative of market power. According to the Guidance [35] market shares only provide a useful first indication, but the Commission needs to interpret market shares in the light of market conditions and in particular dynamics of the market, and to the extent to which the products are differentiated. This is an important point to note as in technology markets over-reliance on market shares might lead to finding dominance too readily. In the recent Microsoft/Skype merger case [36] and Facebook/Whatsapp cases [37] the Commission acknowledged that market shares only provide a limited indication of competitive strength, particularly in consumer communications services due to the fast, dynamic nature of the industry as market shares can change quite rapidly within a short time.

In technology markets where new entrants are in a position to be innovative and compete effectively, it is acknowledged that temporary monopolies could be allowed to emerge with a view to targeting inter-platform competition. This is particularly true when incumbent firms get locked into a particular value network so that they are not able to innovate radically after establishing platform standards. Due to either a propensity to exploit their own installed base or a fear of cannibalising their existing products, or a commitment to established perceptions, the failure of incumbents to introduce radical innovations often creates an opening for a new entrant to introduce a rival information platform [38] . In such situations, market shares do not necessarily reflect the market power attributable to dominant players and their potential to exclude their competitors.

3.2 TYPES OF ABUSE RELEVANT TO DATA PORTABILITY

Dominance or having market power is not a problem as long as an undertaking does not take advantage of its market power, to abuse its market power. Abusive conduct under Article 102 TFEU can roughly be divided into two categories. The first category is 'exploitative abuse', which is conduct that consists of using market power to obtain extra gains from customers such as unfair purchasing and selling prices (Article 102(a)) and by limiting supply to markets (Article 102(b)). The second category is 'exclusionary abuse, which is conduct that attempts to exclude rivals as stated in Article 102(c) (discriminatory conduct) and in Article 102(d) (tie-ins) [39] . Exclusionary abuses are identified more often than exploitative ones [40] .

As the judgment in *Continental Can* [41] clarified, the list of abusive conduct stated in Article 102 TFEU is not exhaustive. Through case law, the Court of Justice of the European Union(CJEU) has expanded the list of abuses to include refusals to supply [42] , margin squeeze [43] , predatory pricing [44] and tying and bundling [45] . In light of the above, it can be argued that a refusal of a dominant firm to enable data portability might be seen as a form of exclusionary abuse as it might drive its competitors out of a specific relevant market and increase market concentration.

3.3 ACCESS TO DATA AS AN ESSENTIAL FACILITY

3.3.1 THE ESSENTIAL FACILITIES DOCTRINE

As mentioned above, Article 102 TFEU articulates only limited types of abuse of dominant position and amongst them no particular reference is made to refusal by a dominant undertaking to deal with a consumer or competitor in the downstream market. While such an abusive conduct might be related to or overlap with the abusive conducts under Article 102 (b) and (c) of the TFEU, most encountered types of 'refusal to deal' have a more distinctive nature, requiring a more characteristic scrutiny. 'Refusal to deal' has emerged as a distinct abusive conduct finding itself a separate place under the Guidance [46] as well as former decisions mostly associated with the essential facilities doctrine.

The essential facilities doctrine is often encountered in relation to refusal to supply (deal) cases and refusal to license cases. The doctrine of the essential facilities originates in US antitrust law [47] . It can be traced back to the *United States v Terminal Railroad Association* case of 1912 [48] . The term essential facility often comes into play where an undertaking seeks access to a physical infrastructure such as a port, airport, railway network or pipeline and when access to the physical infrastructure cannot be reasonably duplicated for technical, legal or economic reasons [49] . In this regard, an obligation regarding 'duty to deal' or 'duty to share essential facilities' arises only if the competitor cannot obtain the goods and services in question elsewhere and cannot build or invent them itself, and unless the facility owner has legitimate business justification for the refusal [50] .

Hence, the 'essentiality' is the most controversial problem in the applicability of the essential facilities doctrine, which adds some difficulties to the traditional 'dominant position' test [51] . The doctrine might also be useful for technology markets and in network industries where a company controls crucial intellectual property or holds data. Hence, it might be argued that if the personal data held by a company is crucial to facilitate market access for other players in a specific industry such as online social networks, online search and online advertising the doctrine of essential facilities might be relevant.

In the EU, the essential facilities doctrine was developed much later than in the US by the application of Article 102 TFEU.

In the seminal case of *Oscar Bronner*, [52] the Court of Justice clarified its position as regards to a new competitor's access to an essential facility. Oscar Bronner was the publisher of a small daily newspaper which accounted for 3.6 per cent of the Austrian daily newspaper market [53] and was enjoying steady growth in new subscriptions and advertisement revenues [54] . On the other hand, Mediaprint was the publisher of two newspapers which together enjoyed 46.8 per cent market share in the Austrian daily newspaper market [55] . Bronner sought access to Mediaprint's established delivery scheme. When Mediaprint refused, Bronner filed a complaint before Austrian courts seeking an order requiring it to

grant access to its delivery scheme for a reasonable payment [56] . The national court referred its preliminary questions to the CJEU.

The CJEU held that provided Mediaprint was found to have a dominant position in the nationwide delivery schemes market and its refusal could amount to an abuse if it satisfied the following criteria cumulatively:

> i) First, refusal was likely to eliminate all competition in the daily newspaper market,
>
> ii) Second, the service must be indispensable for carrying on the entrant's business in that there is no actual or potential substitutes for such delivery,
>
> iii) Third, the refusal must not be objectively justified [57] .

Furthermore, in *Bronner*, the CJEU contended that a product and service is indispensable only if there are no alternative products or services and there are technical, economic or legal obstacles which make it impossible or unreasonable for an undertaking seeking to operate on the downstream market to develop products or services [58] .

The *Bronner* judgment reflects the highest threshold pertinent to the essential facilities doctrine in EU law. Following *Bronner*, in *Magill* [59] , *IMS Health* [60] and *Microsoft case* [61] the CJEU concluded that in order to grant mandatory access, the claimant needs to prove that the data or input requested is essential for the appearance of a new product and there is no other way to obtain or create it [62] .

3.3.2 THE INTERSECTION OF THE ESSENTIAL FACILITIES DOCTRINE AND DATA PORTABILITY

The collection and analysis of user data, including information about the behaviour and preferences of users, enable platforms to optimise the user experience [63] . This drives customer satisfaction and loyalty as customers are prone to use platforms that offer a more personalised experience.

In applying the essential facilities doctrine to the context of data portability, it can be argued that if a dominant company holds specific data that are indispensable for other undertakings to enter a new market, and the dominant company's refusal to transfer that data eliminates all potential competition, then, in the absence of objective justifications, Article 102 TFEU could be relied on. Thus EU competition law emerges as a potential instrument for enforcing data portability objectives in the European Union in an effective way.

While no case involving the essential facilities doctrine and data portability has yet emerged in the EU, in the US, the courts have refused to give mandatory access to specific databases, particularly after the Trinko decision [64] which limited the use of essential facilities doctrine to a great extent.

The *LiveUniverse, Inc. v. MySpace, Inc.* [65] case related to one Social Networking Service (SNS) (MySpace) blocking a user of another SNS (LiveUniverse) from incorporating content from the second SNS's website called vidiLife into their MySpace profile. MySpace's deletion of all references to vidiLife and preventing its users from incorporating any kinds of such extensions was claimed by LiveUniverse to be contrary to US antitrust law. The District Court dismissed the alleged claims of exclusionary conduct, referring to the lack of a duty to deal which according to the Court requires existence of a voluntary agreement as defined in

Supreme Court's *Trinko* decision *(Verizon Communications Inc. v. Law Offices of Curtis V Trinko, LLP)* . The District Court's dismissal as upheld by the Ninth Circuit affirmed Myspace's freedom of product design as well as its right to deal within the meaning of Section 2 of the Sherman Act [66] .

Facebook v. Power Ventures Inc. [67] related to Power Ventures' attempt to extract data (all kinds of social networking contacts of users) from SNS platforms including Facebook and display them on its own platform called Power.com. In the face of Facebook preventing such an attempt and suing Power Ventures for breach of its terms of service, Power Ventures filed a counter case against Facebook based on exclusionary conduct [68] . However, Power Ventures' claims were not affirmed by the District Court which considered lack of interoperability outside the scope of Section 2 liability, referring to Facebook's 'right to manage access to and use of its website' [69] .

In *PeopleBrowsr v. Twitter* [70] , the dispute stemmed from PeopleBrowsr asking Twitter to grant it (full firehose) access to Twitter data to be able to offer analytics services and being denied this request. PeopleBrowsr filed a case with the claims based on private law and California's unfair competition law gave a result of a 'temporary restraining order' imposed on Twitter [71] . Twitter attempted to carry on the case at the federal (antitrust) level but this failed [72] . The parties eventually settled the case by agreeing that PeopleBrowsr could continue full firehose access until 2013 [73] . As the case ended with a settlement, it is unclear whether Twitter would have been obliged to give *PeopleBrowsr* full access to its data under US federal or state antitrust law.

US antitrust law and principles, particularly after the *Trinko* decision [74] , took a divergent path from mandatory access obligations, whether through the essential facilities doctrine or other tools (e.g. intent test, market leverage). Thus, proving the 'indispensability' or 'essentiality' of the requested input often poses the main difficulty for the plaintiffs to overcome. This is more persuasive in the ICT markets which reveal temporary monopolies within the sense of 'destructive' or in other words 'Schumpeterian' innovations. Less dependence on the incumbent platforms, reduction of total costs (e.g. thanks to the simplification of network architecture and capacity increases), and applicability of enhanced software applications by service providers may make economies of scale achievable and bottlenecks less relevant in the Internet ecosystem.

Platforms such as Google may prove to represent a counter thesis to this. The quality of search results and the targeting of advertising using Google Search relies to a large extent on personal data - i.e. the user's previous searches and search behaviour using the search engine - and also data shared through other services on the same platform such as Google Photos (with e.g. location data), Gmail (with email text analysis), Google Maps (travel data) and YouTube (interest data). Arguably Google's possession of this data amounts to a significant competitive advantage, one of such magnitude that it cannot realistically be replicated by other players in the market, even by digital giants such as Apple or Microsoft with their significant resources.

The portability of users' search histories and search behaviours in particular lies at the heart of this, and clearly at the intersection of both data and competition laws. It is worth noting that Google user search history can already be exported using Google Takeout. However it is not clear how many users make use of this opportunity. Arguably, users are uninterested in pure data export, as it is a complex and time-consuming process, with inherent uncertainty, as the data transferred may not be utilised by other data controllers due to technical and architectural constraints. In this respect, controller-to-controller data portability is crucial to

safeguard the right to data portability - and thereby effective competition in platform based markets. The success of the GDPR in the context of data portability and platforms such as Google may rest on the ability to enforce effective controller-to-controller portability rather than simple export functionality.

As mentioned above, in the EU there has not been any precedent in which access to a database of personal data was seen as essential for the operation of a particular service where it would be commercially impossible for a competitor to operate without that personal data. Given the stringent nature of the essential facilities doctrine, it would be relatively difficult for an undertaking to demonstrate why they cannot develop their own database of personal information without access to the dominant competitor's data. However, as the below case law demonstrates, given the willingness of the European Commission and national competition authorities to take a closer look at markets that collect and process personal data, it is likely that there will be cases where refusal to give access to a specific data set could be considered an essential facility.

4. ANALYSIS OF COMPETITION CASES RELATING TO DATA PORTABILITY AND THE USE OF PERSONAL DATA

4.1 GOOGLE CASE

An important case involving data portability is the pending competition investigation into Google.

In February 2010, several vertical search engines, such as Foundem, Ciao and ejustice.fr (a French legal search engine) filed a complaint before the European Commission. These three complaints focused on abuse of dominance: that Google used its dominant search engine and its 'Universal Search Service' [75] to promote its own services whilst discriminating as well as demoting the search rankings of competing websites and other vertical search engines among its unpaid and paid search results [76] . In addition to its natural (organic) search results, Google also operates vertical search services which offer a specific search function for a category of products such as services and information. According to rival vertical search engines, Google prioritises its own vertical search services such as Google News and Google Shopping at the expense of its rivals' vertical search engines.

In addition to the first complaint in relation to Google's alleged prioritisation of its own services, in the scope of its investigation the European Commission is also investigating the following:

i. Whether Google has imposed exclusivity obligations on advertising partners, hindering them from placing certain types of competing adverts on their websites, as well as on computer and software vendors with the aim of foreclosing competition for competing search tools,
ii. Whether Google has restricted the portability of online advertising data to competing online advertising platforms and
iii. Whether Google uses third party content, mainly websites whose content competes with its offerings whilst reducing competitors' incentives to invest in creating original content, to the detriment of consumers [77] .

As of April 2016, the Commission is also investigating whether Google is abusing its dominant position on the mobile devices market by imposing restrictions on Android device manufacturers and mobile network operators [78] .

For the purpose of this paper, attention will only be paid to Google restricting the portability of data from its AdWords platform to other competing online advertising platforms. The Commission is concerned that Google imposes contractual restrictions on software developers which prevent them from offering tools that would enable the seamless transfer of search advertising campaigns across Google's AdWords to other search advertising platforms [79] . In other words, according to the Commission, Google needs to refrain from exclusionary contracts which hinder data portability. Needless to say, such restriction is likely to lock-in advertisers to Google's online advertising platform and have an adverse effect on other online advertising platforms such as Bing's advertising platform. As the costs of recreating an online advertising campaign are high, most small and medium-sized companies will only use Google's AdWords platform. As a result, other advertising platforms are likely to be excluded from the online advertising market.

In order to resolve the competition law concerns concerning data portability, Google proposed that it would cease any written or unwritten obligations in its AdWords API terms and conditions that hindered advertisers from transferring and managing search advertising campaigns from Google's AdWords to other competing search advertisement services. On 14 July 2016, the Commission initiated antitrust proceedings against Google [80] . It is not clear whether the above remedy proposed by Google in relation to data portability will be considered an effective remedy.

It should be noted that Google was subject to a relatively similar antitrust investigation in the United States by the Federal Trade Commission (FTC) where in relation to the data portability concerns Google agreed to further facilitate the portability of AdWords data across other search platforms. However, as pointed out by Heiner, the FTC did not seek any feedback as to the effectiveness of this remedy, hence it remains to be seen whether the proposed remedy by Google will be sufficient to allow the smooth transfer of data from Google's AdWords platform to other advertising platforms [81] .

The *Google* case demonstrates the importance of the EU Commission in facilitating data portability in order to avoid consumer lock-in in concentrated markets such as online advertising and online search. As discussed earlier, Google, as a search engine, posses a vast amount of personal data such as user search history, search results and search behaviours, which enables it to deliver relevant and high quality search results. Arguably, by not sharing this data with its competitors Google prevents other search engines such as Bing from effectively competing with it. As suggested by Lianos and Motchenkova, if Google were to share search results with its competitors, this may enable its competitors to provide search results of at least similar degree of relevance to the consumers' questions [82] .

The Google case also illustrates that restrictions on data portability may qualify as an abuse of dominance under Article 102 TFEU(b) if it can proved that the dominant company limit markets and technical development to the prejudice of consumers [83] .

Finally, this case is significant as it clearly shows that Article 102 TFEU can expand the scope of the right to data portability under the GDPR by looking after the interest of businesses which normally cannot take advantage of the right to data portability under the GDPR.

4.2 FACEBOOK

Another interesting, recent case is a German case that concerns Facebook. On May 2016, the Bundeskartellamt, the German competition authority, started investigating whether Facebook abuses its dominant position on social networks in the German market. The Bundeskartellamt alleged that Facebook's terms and conditions of service regarding how it makes use of user's personal data may amount to abuse of dominance in the social networking market [84] . Like any online service, in order to use Facebook consumers need to agree to its terms and conditions prior to using its services. According to the Bundeskartellamt, Facebook is allegedly imposing unfair trading terms on consumers contrary to Article 102 TFEU as consumers are not in a position to understand the scope and amount of data captured by the company for advertising and other purposes. Arguably, this can be seen as an exploitative abuse under Article 102(a) if it can be established that Facebook uses its market power to obtain extra gains from online users who are not in a strong position to negotiate the terms and conditions of Facebook's service.

Andreas Mundt, President of the Bundeskartellamt, stated the following on the case:

> Dominant companies are subject to special obligations. These include the use of adequate terms of service as far as these are relevant to the market. For advertising-financed Internet services such as Facebook, user data are hugely important. For this reason it is essential to also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected. [85]

This was the first case in the EU where a dominant company was subject to a competition probe for allegedly infringing data protection laws. It must be noted that in January 2016 the European Competition Commissioner Margrethe Vestager stated that dominant technology platforms that harvest vast amounts of data might be considered in breach of EU competition rules if they are using this data to drive their competitors out of the market [86] . The Commissioner pointed out that if a dominant company's use of data was bad for competition, thus potentially outweighing any benefits to customers such as reduced costs, the Commission could step in to restore a level playing field [87] .

The *Facebook* case and the above statement of the Competition Commissioner demonstrate the interplay between data protection laws and competition law and how failure to comply with the relevant provisions of the GDPR, including the right to data portability, is likely to trigger competition law probes at EU level and in several EU member states. It is possible that in the future, online platforms such as Google, Facebook, Amazon, Apple which harvest a vast amount of personal data might be subject to competition investigations if they fail to comply with the GDPR, providing that such failure has an adverse effect on consumers and/or hinders market entry for potential competitors.

5. CONCLUSION

The right to data portability is no doubt a key concern for online users as well as for companies that wish to have a level playing field. Businesses cannot resort to Article 20 of the GDPR as the right to data portability is only available to living and identifiable individuals. Nevertheless, EU competition law and particularly Article 102 TFEU can be used to enforce data portability across platforms, thus filling this gap in the GDPR.

This article finds that the right to data portability under Article 20 of the GDPR might not deliver the intended results due to its ambiguity and due to the inherent limitations contained therein such as the rights and freedoms of other data subjects. As noted in Section 2, in its current form the right to data portability may create disproportionate costs for small and medium sized enterprises, compromise valuable proprietary information and intellectual property rights and lead to privacy and security breaches. In order to alleviate these concerns, the Article 29 Working Party should provide concrete guidelines explaining how to interpret key terms in Article 20 of the GDPR, such as what is meant by technically feasible, what is meant by data provided by the data subject himself/herself, as well as clarifying the delimitations of the right to data portability. Clear guidelines may encourage industry players to introduce solutions based on commonly accepted practices such as well documented APIs or de facto data standards and/or protocols, thus enabling controller to controller data transfer.

This article also points out that in order to ensure an effective right to data portability, the transfer of data from one controller to another is far more significant than the transfer of data from a controller to an individual, as such manual export and import of data could be well beyond the average user's technical ability and there is no clarity as to whether the exported data can be used by another data controller. Thus, the forthcoming guidelines should concentrate on how to strengthen and encourage controller-to-controller data portability. In this regard, further research is needed to determine whether users would prefer controller-to-controller data transfer and how such transfer could be made simple and technically feasible, such as by clicking a button or by following a few simple steps.

As discussed under Section 3 and Section 4, the main difference between the GDPR and competition rules is that EU competition rules only apply to dominant service providers whilst the rules contained in the GDPR can be enforced against all data controllers irrespective or their size and market shares. The right to data portability has many implications such as facilitating market access, preventing high switching costs and alleviating network effects that threaten potential competition in a marketplace. These implications necessitate this individual right to be analysed in the context of competition law rules and precedents. As Section 3 and Section 4 highlights, EU competition rules, particularly Article 102 TFEU, and the essential facilities doctrine can offer sensible solutions by enforcing mandatory data portability, where the data owned by an incumbent is necessary for the appearance of a new product or service and there is no other possibility for another competitor to obtain the data to perform its services and compete with the dominant undertaking.

In order to ensure legal certainty with regard to data portability, the Article 29 Working Group, the European Data Protection Supervisor, and the Data Protection agencies in the member states should assist the data controllers in their compliance efforts. Arguably, in limiting the potential harmful impact of the data portability provision for small and medium-sized enterprises some lessons can be drawn from EU competition law. As explained above, Article 102 TFEU only applies to dominant companies with significant market power. In a similar vein, the European Merger Regulation [88] is only applicable to mergers with a community dimension and where the undertakings have a significant turnover [89] . Perhaps, in order to alleviate the potentially harmful impacts of the right to data portability on small and medium-sized enterprises, undertakings with a limited market share or with an insignificant turnover can be exempted from data portability requirements.

In order to have effective data portability within the EU that covers all stakeholders, including users and businesses, the implementation of the GDPR must be in harmony with competition

law and other relevant legislation such as consumer protection laws. This will require cooperation between the relevant competition authorities, the European Data Protection Supervisor, national data protection agencies and sector-specific regulatory authorities where necessary.

---

[1] Dr Aysem Diker Vanberg is a Senior Lecturer at Anglia Ruskin University.

[2] Dr Mehmet Bilal Ünver is a Doctoral Researcher at Anglia Ruskin University.

[3] The authors would like to thank the reviewers for their invaluable comments. The research assistance of Nicole St Hilaire is also gratefully acknowledged.

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

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[6] See for instance, Alexander Brown and Clare Adam, 'The draft regulation -does every cloud have a silver lining? (2012) 12(4) P& DP 9, Winston J. Maxwell, 'Data Privacy: the European Commission pushes for total harmonisation' (2012) 18(6) CTLR 175.

[7] See for instance, Nick Graham, 'Data protection and privacy' (2012) 98 (Aug) COB 1, Sana Khan, 'Practitioner's insight into the new EU Data Regulation (2016) 5(1) Comp& Risk 6; Eduardo Ustaran, 'EU General Data Protection Regulation: things you should know' (2016) 16(3) P & DP 3 ; Anita Bapat, ' The new right to data portability' (2013) 13(3) P & DP 3 and Francoise Gilbert,' European data protection 2.0: new compliance requirements in sight-what the proposed EU data regulation means for US companies' (2001) 28(4) Santa Clara High Technology Law Journal 815.

[8] In this article the terms 'individual' , 'consumer', ' user' and 'data subject' are used interchangeably to refer to a 'data subject'. According to Article 4 of the GDPR a 'data subject' is an identifiable natural who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[9] Gabriela Zanfir, 'The Right to Data Portability in the Context of Data Protection Reform' (2012) 2(3) International Data Privacy Law 149.

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

[11] Anita Bapat ' The new right to data portability' (2013) 13(3) P & DP 3.

[12] Fablab Workshop is a workshop organised by the Article 29 Working Party in Brussels on July 26, 2016., with more than 90 participants including 40 representatives from Data protection Authorities. Amongst other issues the participants have discussed the issues relating to data portability. See 'Fablab GDPR/from concepts to operational toolbox,DIY' Results of the discussion' (2016) available at :< http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf > accessed 17 November 2016.

[13] Fablab 'GDPR/from concepts to operational toolbox,DIY' Results of the discussion (2016) available at :< http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf > accessed 17 November 2016.

[14] Inge Graef, Jeroen Verschaleken, Peggy Valcke, 'Putting the right to data portability into a competition law perspective' (2013) Law: The Journal of the Higher School of Economics, Annual Review 4. Available at SSRN: < http://ssrn.com/abstract=2416537>accessed 17 November 2016.

[15] Inge Graef, Jeroen Verschaleken, Peggy Valcke, 'Putting the right to data portability into a competition law perspective' (2013) Law: The Journal of the Higher School of Economics, Annual Review 4. Available at SSRN< http://ssrn.com/abstract=2416537>accessed 12 November 2016.

[16] Barbara Engels, 'Data portability amongst online platforms' (2016) 5(2) Internet Policy Review 4. <http://policyreview.info/articles/analysis/data-portability-among-online-platforms> accessed 17 November 2016.

[17] Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335.

[18] Laurits R Christensen, Andrea Colciago, Federico Etro, Greg Rafaert, 'The Impact of the Data Protection Regulation in the EU' (2013) European Financial Review 72.

[19] Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335, 379.

[20] John Bowman, 'New UK Minister's Data Protection To-Do List' (2015) <https://iapp.org/news/a/new-uk-ministers-data-protection-to-do-list/> accessed 28 July 2016.

[21] True Fit is footwear and apparel's discovery platform, which uses personal data obtained from users to enable them to find a better fit for clothing and footwear. The information on True Fit is available at <truefit.com> accessed 17 November 2016.

[22] Article 29 Data Protection Working Party, ' Statement on the 2016 Action Plan for the implementation of the General Data Protection Regulation' 2 February 2016< http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf > accessed 17 November 2016.

[23] Anita Bapat, 'The new right to data portability' (2013) 13(3) P & DP 3, 4.

[24] Final report of the Federal Trade Commission Advisory Committee on Online Access and Security 19-25

(May 15, 2000) <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf> accessed 28 July 2017; see also Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) Maryland Law Review 335, 374.

[25] The GDPR, Recital 68.

[26] Urs Gasser, 'Interoperability in the digital ecosystem' (2015) Berkman Center Research Publication No. 2015-13 12. Available at SSRN <http:// ssrn.com /abstract=2639210> accessed 17 November 2016.

[27] Former Competition Commissioner Almunia, 'Competition and personal data protection' Speech delivered at the Privacy Platform Event: Competition and Privacy in Markets of Data in Brussels on 26 November 2012,< http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm > accessed 17 November 2016.

[28] Carl Shapiro and Hal R. Varian, *Information Rules, A strategic guide to the network economy* (1999) Boston, MA.

[29] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326.

[30] Case 27/76 *United Brands* [1978] ECR 207, par.65.

[31] Case 85/76 *Hoffman-La Roche & Co AG v Commission of the European Communities* (1979) ECR-4361. (Hereinafter *Hoffman La Roche*)

[32] *Hoffman La Roche* paragraph. 41.

[33] Mario Monti, 'Market Definition as a Cornerstone of EU competition Policy' Workshop on Market Definition, Helsinki, 5 October 2001.

[34] See Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, C(2009) 864 final, Brussels, 9.2.2009, < http://ec.europa.eu/transparency/regdoc/rep/3/2009/EN/3-2009-864-EN-F-0.Pdf. >accessed 28 July 2016.

[35] See Guidance, para.13.

[36] Case COMP/ M.6281, *Microsoft/Skype*, October 7, 2001, C (2011)7229, para.78.

[37] Case COMP/ M.7217 *Facebook/Whatsapp*, October 3, 2014, C(2014) 7239, para 99.

[38] Philip Weiser, 'The Internet, Innovation, and Intellectual Property Policy' (2003) Vol 103 Columbia Law Review 588.

[39] Steven Anderman and Hedvig Schmidt, *EU Competition Law and Intellectual Property Rights: The Regulation of Innovation* (2nd edition, Oxford University Press, 2011) 34.

[40] Kevin Coates, *Competition Law and Regulation of Technology Markets* (Oxford University Press 2011) 27.

[41] Case 72/71 *Continental Can Co. Inc.,* (1972) OJ L7/ 25.

[42] On refusal to supply see for instance, *Case 6 and 7/73, Istituto Chemioterapico Italiono SpA and Commercial Solvents Corp v. Commission* [1974] ECR 223 and Sealink/ BI Holyhead: Interim Measures [1992] 5 CMLR 255; Case C-418/01 *IMS Health GmBH & Co KG* [2004] ECR 1-5039 and Case T-201/4 *Microsoft v . Commission* [2007} ECR II- 3601.

[43] On margin squeeze see for instance, Case T-336/07 *T elefónica and Telefónica de España v. European Commission,* [2012] 5 CMLR 931.

[44] On predatory pricing see for instance, Case C-62/86 Akzo Chemie BV v. Commission [1991] ECR I-3359 and Case C-209/10 Post Danmark A/S v. Konkurrencerådet [2012] ECR I-0000.

[45] On technical bundling see for instance Case T-201/4 *Microsoft v. Commission* [2007} ECR II- 3601.

[46] See Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, C(2009) 864 final, Brussels, 9.2.2009, http://ec.europa.eu/transparency/regdoc/rep/3/2009/EN/3-2009-864-EN-F-0.Pdf.

[47] On the essential facilities doctrine under U.S. Law see for instance, Philip Areeda, 'Essential Facilities: An Epithet in Need of Limiting Principles' [1989] 58 Antitrust L.J. 841; Abbott Lipsky& Gregory Sidak, 'Essential Facilities' (1999) 51 Stanford Law Review1187; Robert Pitofsky, Donna Patterson & Jonathan Hooks, 'The Essential Facilities Doctrine under U.S. Antitrust' (2002) 70 Antitrust Law Journal 443.

[48] The case *(United States v Terminal Railroad Association 224 US 383 (1912)* concerned access to a bridge to be operated by a joint venture comprising fourteen out of the twenty-four rail companies. Thus there was concern that the joint venture could exclude the access of the remaining ten rail companies to the bridge.

[49] Laurent Garzaniti, 'Application of the EU Competition rules to the Telecommunications, Broadcasting and Internet sectors' in Laurent Garzaniti and Matthew O'Regan (eds.)*Telecommunications, Broadcasting and the Internet* (3 rd edn, Thomson Reuters Legal Limited 2010) Part II 458.

[50] John Temple Lang, 'The Principle of Essential Facilities in European Community Competition Law - The Position since Bronner - Notes for a lecture' September 2000, Copenhagen, 2.

[51] In fact, additional questions arise in this context. First and foremost, in essential facilities cases, there are two related markets namely the market for the supply of the needed input (upstream market), and the market for the goods or services produced via access to the relevant input (downstream market). Beyond this, refusal to supply the necessary input with no objective justification is sought as well as the access-denied input being essential for the competition in the downstream market.

[52] Case C-7/97 *Oscar Bronner GmBH & Co KG v. Mediaprint* [1998] ECR I- 7791 (hereinafter Oscar Bronner)

[53] Oscar Bronner para. 4.

[54] Oscar Bronner para. 67.

[55] Oscar Bronner para. 6.

[56] Oscar Bronner para 8.

[57] Oscar Bronner para. 41.

[58] Oscar Bronner paragraphs 44-45.

[59] Joined Cases C-241/91 and C-242/91[1995] ECR I- 743.

[60] Case C-418/01 [2004] ECR I-5039

[61] Case T-201/4 *Microsoft v .Commission* [2007} ECR II- 3601.

[62] Josef Drexl, Reto M.Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter, Gintare Surblyte and Klaus Wiedermann, ' Data Ownership and Access to Data Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate' (2016), 9.
< http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf > accessed 17 November 2016.

[63] Inge Graef, Sih Yuliana Wahyuningtyas and Peggy Valcke, 'Assessing data access issues in online platforms' [2015]] 39(5) *Telecommunications Policy*, 375, 378.

[64] *Verizon Telecommunications Inc.* v. *Law Offices of Curtis V. Trinko*, LLP 540 U.S. 398, 2004 (*Trinko* judgement).

[65] LiveUniverse, Inc. v. MySpace, Inc., No. CV 06-6994 AHM (RZx), 2007 WL 6865852, (C.D. Cal. June 4, 2007).

[66] LiveUniverse, Inc. v. MySpace, Inc., 304 Fed. Appx. 554 (9th Circ. December 22, 2008).

[67] Facebook, Inc. v. Power Ventures, Inc., No. C 08-5780 JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010).

[68] Facebook, Inc. v. Power Ventures, Inc., paragraphs 13-14. According to Power Ventures's claim Facebook had been engaged in exclusionary conduct by allowing its users to use their Facebook login information to access other service providers including Gmail, AOL, Yahoo!, Hotmail while preventing its competitors from doing the same.

[69] Facebook, Inc. v. Power Ventures, Inc., paragraphs 13-14

[70] PeopleBrowsr (2013) PeopleBrowsr, Inc. Et al. v. Twitter, Inc., No. C-12-6120 EMC, 2013 WL 843032 (N.D. Cal. March 6, 2013).

[71] PeopleBrowsr (2012) PeopleBrowsr wins temporary restraining order compelling twitter to provide firehose access. 28 November 2012.< http://blog.peoplebrowsr.com/2012/11/peoplebrowsr-wins-temporary-restraining-order-compelling-twitter-to-provide-firehose-access/> accessed 27 July 2016

[72] PeopleBrowsr (2013) PeopleBrowsr, Inc. Et al. v. Twitter, Inc., No. C-12-6120 EMC, 2013 WL 843032 (N.D. Cal. March 6, 2013).

[73] PeopleBrowsr. (2013) PeopleBrowsr and Twitter settle Firehose dispute. 25 April 2013.<http://blog.peoplebrowsr.com/2013/04/peoplebrows

r-and-twitter-settle-firehose-dispute/> accessed 27 July 2016.

[74] *Verizon Telecommunications Inc.* v. *Law Offices of Curtis V. Trinko*, LLP 540 U.S. 398, 2004 (*Trinko* judgment).

[75] Universal Search was introduced by Google in 2007. Universal Search returns a variety of information about the search query as opposed to traditional text results. As an example, when one searches for Michael Jackson, Universal Search not only brings information about Michael Jackson, but also brings images, news, local listings, shopping, video, blog posts and so on. Google calls this service 'blending', whilst others call it bundling, as Universal Search places Google's own services such as YouTube results and Google News in prominent positions within search results.

[76] Google's search engine provides two types of results; the first one is "unpaid" search results which are sometimes also referred to as "natural", "organic" or "algorithmic" search results, and the second is "paid third party advertisements", shown at the top and/or at the right hand side of Google's search results page, often referred to as "paid" search results or "sponsored links".

[77] IP/10/1624, Press Release, 'Antitrust: Commission probes allegations of antitrust violations by Google", 30 November 2010.

[78] See European Commission Press Release 'Antitrust Commission sends Statement of Objections to Google on Android operating system and applications' 20 April 2016 < http://europa.eu/rapid/press-release_IP-16-1492_en.htm > accessed 17 November 2016.

[79] Competition Policy Statement of VP Almunia on the Google antitrust investigation, 21 May 2012, SPEECH 12/372 < http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm > accessed 17 November 2016.

[80] Commission, 'Google Opening of Proceedings' dated 14 July 2016 available < http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14009_3.pdf > accessed 17 November 2016.

[81] D. Heiner 'The FTC and Google: A missed Opportunity' 3 January 2013,< http://blogs.microsoft.com/on-the-issues/2013/01/03/the-ftc-and-google-a-missed-opportunity/#sm.00000wauh0wkddfiwtjr7zy307ogy > accessed 14 November 2016.

[82] Ioannis Lianos and Evgenia Motchenkova 'Market Dominance and Search Quality in the Search Engine Market ' (2013) 9(2) Jnl of Competition Law & Economics 419, 455.

[83] For an extensive discussion on this point see, Damien Geradin and Monika Kuschewsky 'Competion Law and Personal Data: Preliminary Thoughts on a Complex Issue, 11 Available at SSRN < https://ssrn.com/abstract=2216088 or http://dx.doi.org/10.2139/ssrn.2216088 > accessed 17 November 2016.

[84] Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules,2 March 2016 <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 17 November 2016.

[85] Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules,2 March 2016 <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 27 June 2016.

[86] Margrethe Vestager,' Competition in a big world' Speech delivered at DLD 16, Munich 17 January 2016< https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big-data-world_en. > accessed 17 November 2016.

[87] Margrethe Vestager,'Competition in a big world' Speech delivered at DLD 16, Munich 17 January 2016< https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big-data-world_en> accessed 17 November 2016.

[88] Council Regulation (EC) 139/2004 on the control of concentrations between undertakings (EU Merger Regulation) [2004] OJ L24/1.

[89] According to Article 2 of The EU Merger Regulation, the Regulation is applicable to mergers with a community dimension.

A concentration has a Community dimension where:

(a) the combined aggregate worldwide turnover of all the undertakings concerned is more than EUR 5000 million; and

(b) the aggregate Community-wide turnover of each of at least two of the undertakings concerned is more than EUR 250 million, unless each of the undertakings concerned achieves more than two-thirds of its aggregate Community-wide turnover within one and the same Member State.