

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

How to attribute the right to data portability in Europe: A comparative analysis of legislations

Barbara Van der Auwermeulen *

Faculty of Law, University of Vienna, Austria

A B S T R A C T

Keywords:

General Data Protection Regulation
Data portability
Competition law
US antitrust
Online services
Personal data
Privacy

The number of online services is constantly growing, offering numerous and unprecedented advantages for consumers. Often, the access to these services requires the disclosure of personal information. This personal data is very valuable as it concedes significant advantages over competitors, allowing better answers to the customer's needs and therefore offering services of a better quality. For some services, analysing the customers' data is at the core of their business model. Furthermore, personal data has a monetary value as it enables the service providers to pursue targeted advertising. Usually, the first companies who provide a service will benefit from large volumes of data and might create market entrance barriers for new online providers, thus preventing users from the benefits of competition. Furthermore, by holding a grip on this personal data, they are making it more expensive or burdensome for the user to shift to a new service. Because of this value, online services tend to keep collected information and impede their users to reuse the personal data they have provided. This behaviour results in the creation of a lock-in effect. Upcoming awareness for this problem has led to the demand of a right to data portability. The aim of this paper is to analyse the different legislative systems that exist or have been recently created in this regard that would grant a right to data portability. Firstly, this article draws up the framework of data portability, explaining its origin, general aspects, advantages as well as its possible downfalls. Secondly, the core of the article is approached as the different ways of granting data portability are analysed. In this regard, the possible application of European Competition Law to prohibit restrictions to data portability is examined. Afterwards, an examination of the application of U.S. Antitrust Law is made to determine whether it could be a source of inspiration for European legislators. Finally, an analysis of the new General Data Protection Regulation is made with respect to the development of data portability throughout the European legislative procedure. This article makes a cross-examination of legislations, compares them with one another in order to offer a reflection on the future of portable data in Europe, and finally attempts to identify the best approach to attribute data portability.

© 2016 Barbara Van der Auwermeulen. Published by Elsevier Ltd. All rights reserved

* Universität Wien, Universität Ring 1, 1010 Vienna, Austria.

E-mail address: barbara.vdauwermeulen@gmail.com.

<http://dx.doi.org/10.1016/j.clsr.2016.11.012>

0267-3649/© 2016 Barbara Van der Auwermeulen. Published by Elsevier Ltd. All rights reserved

1. Introduction

Today, there exist a number of online services, which provide numerous advantages for consumers, offering social connections, innovations, and efficient problem solving like never before in the past.¹ Access to these online services often requires the disclosure of personal information. This personal data is very valuable as it concedes significant advantages over competitors, allowing better answers to the customer's needs and therefore offering services of a better quality.² For some services, analysing the customers' data is at the core of their business model. Furthermore, personal data has a monetary value as it enables the service providers to pursue targeted advertising.³ Usually, the first companies who provide a service will benefit from large volumes of data and might create market entrance barriers for new online providers, thus preventing users from the benefits of competition.⁴ Furthermore, by holding a grip on this personal data, they are making it more expensive or burdensome for the user to shift to a new service. Because of this value, online services tend to keep collected information and impede their users to reuse the personal data they have provided. This behaviour results in the creation of a lock-in effect.

Upcoming awareness for this problem has led to the demand of a right to data portability. The general aspects of this right as well as the advantages and downfalls it generates are introduced in this contribution in order to provide a general overview of the topic.

The focus of this contribution resides nevertheless in analysing the different legislative systems in order to identify the best approach to grant data portability. In this regard, an analysis of the first possible legislative way of attributing data portability is made, namely through European Competition Law. This part of the contribution does not aim at enunciating all the European Competition Law principles but focuses on the possible enforceability of data portability through competition law. Because this constitutes many difficulties, an analysis of U.S. antitrust law is made to see if there are principles that can be useful to European Competition Law.

Subsequently, privacy regulation will be examined. In 2012, the European Commission (EC) revealed its intention to include a right to data portability in its proposal for a General Data

Protection Regulation (GDPR).⁵ Since then, many changes have been made in this regard. The way the European Commission proposes to attribute this right, the modifications made by the European Parliament (EP) and the Council of the European Union as well as the concerns raised by the integration of data portability in the GDPR are discussed in this contribution. This is finally followed by a reflection on the future of data portability in Europe and an attempt to identify the best approach to attributing data portability.

2. Data portability: origin, general aspects, advantages and drawbacks

2.1. Origin

The debate about data portability originated with the Internet users' need to transfer data they had been building up such as e-mail, friends' lists or address books from one service to another service.⁶ Later on, it appeared that next to the primary aim of enabling users to easily move their data, it was also regarded as a mechanism that was necessary in order to prevent unfair competition and make data protection of individuals effective.⁷ In 2007, a first claim for freedom and control of personal data was brought forward through a 'Bill of Rights for Users of the Social Web'.⁸ Although it had no legal force, it was a first step to a right for data portability. A few months later, the 'Data Portability Project'⁹ was founded with the ambition to discuss and work on solutions to unconstrained data portability. The success was imminent and one year later, Google and Facebook became members of the Project.¹⁰

At that time, data portability was not considered legislatively by the European Union's institutions and constituted a new challenge in the perspective of protection of personal data.¹¹ Indeed, the already existing directive 95/46/EC¹² does not cope with the new challenges for the protection of personal data. Measuring the importance of the subject, the European

¹ European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (Preliminary Opinion) (March 2014) 6 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf> accessed 10 November 2015.

² Damien Geradin & Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (February 12, 2013) SSRN 1, 2 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088> accessed 10 November 2015.

³ *ibid.*

⁴ *ibid.*

⁵ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

⁶ Gabriela Zafir, 'The right to data portability in the context of the EU data protection reform' Vol 2(3) International Data Privacy Law, Oxford University Press 149.

⁷ *ibid.*

⁸ Joseph Smarr, Marc Canter, Robert Scoble, Michael Arrington and others, 'A Bill of Rights for Users of the Social Web' ([Template.org](http://www.template.org), 4 September 2007) <http://www.template.org/?page_id=599> accessed 21 May 2016.

⁹ See <<http://dataportability.org/>> accessed 21 May 2016.

¹⁰ Duncan Riley, 'Facebook, Google and Plaxo Join the Data Portability Workgroup' (*Techcrunch*, 8 January 2008) <<http://techcrunch.com/2008/01/08/this-day-will-be-remembered-facebook-google-and-plaxo-join-the-dataportability-workgroup/>> accessed 21 May 2016.

¹¹ Zafir (n 6) 149.

¹² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31.

Commission organised a debate in 2010 in order to discuss the reconsideration of the existing legal framework in the domain of data protection in a way for it to confront the contemporary challenges of the Web 2.0.¹³ Those debates led to a proposal for a General Data Protection Regulation¹⁴ in which the subject of data portability is one of the discussed points.

2.2. General aspects of the data portability right

The idea of data portability is to attribute the online users, the right to keep control over their data by being able to transfer and share the latter.¹⁵ The co-founder of the Data Portability Project, Chris Saad, describes it as the opportunity for “a borderless experience, where people can move easily between network services, reusing data they provide while controlling their privacy and respecting the privacy of others”.¹⁶ In other words, data portability would allow users of online services the liberty to move the data they have been building up, from one service to the other. This would increase the movement between online services as the entrant’s procedure would be greatly facilitated and accelerated. Users who are willing to subscribe to a new online service would therefore not have to manually enter all their information, but could transfer it from a similar online service on which they already have all the relevant information. Ideally, this transfer would have to be possible in a few clicks and without hindrance. An example thereof would be the probability for a user of eBay, to transfer its seller profile to a new online auction service.

The European Data Protection Supervisor compares the right to data portability with “number portability”.¹⁷ The latter concedes the right of telephone users to keep their telephone number, regardless of the organisation providing services.¹⁸ In fact, before the Universal Service Directive¹⁹ was implemented, telephone users could not maintain their telephone number when they shifted to a competing service provider. The consequence of losing their telephone number created such an encumbrance on the part of the users that they would simply

stay with their initial service provider, creating a lock-in effect.

Finally, portability is closely connected to interoperability.²⁰ This is a broad term that encompasses the different aspects that have to be considered in order for services or systems of different sources to collaborate.²¹ In fact, systems have to be able to interoperate in order for data to be moved and reused from one provider to another, disregarding the fact that systems may be different.²² According to Chris Saad, co-founder of the Data Portability Project, “Interoperability means that irrespective of who is providing or receiving the data, it should be provided in such a way that is agreed upon by the community so that the implementation is consistent irrespective of parties participating in the transaction”.²³ In other words, it is a requirement that the service providers have to meet in order to make data portability possible. The requirement is that systems of different system providers have to be able to act in conjunction with one another so as to ease the transfer of the data uploaded on one site to the other and this in an easy and fast way for the user.²⁴ It could be regarded in this context as “a synonym of integration”.²⁵

2.3. Advantages and downfalls of data portability

Data portability is a contemporary subject that causes controversy. The aim of this section is to discuss the advantages as well as the potential downfalls of data portability. As the advantages seem relatively clear, it cannot be excluded that granting a right to transfer all your personal data without hindrance, might have negative consequences.

2.3.1. The advantages of data portability

In the first place, data portability benefits the users of online services. It would allow them, as mentioned before, to transfer their personal information easily from one service to another and therefore be free to choose the service that is the most suitable to their needs. Furthermore, by enabling users to stay in control of their information, the service providers will create a more user-friendly online environment in which the users will trust.²⁶ Another advantage for the user concerns its consumer protection. By creating barriers to the transfer of personal data to a competitor that is not necessary for providing their service, the service providers harm consumers and distort

¹³ Commission, ‘A comprehensive approach on personal data protection in the European Union’ (Communication) COM (2010) 609 final.

¹⁴ Proposal for a General Data Protection Regulation, 11 final.

¹⁵ Loek Essers, ‘Dataportabiliteit: “sluit je bij ons aan of verlies”’, (Webwerelds, 4 April 2008) <<http://webwereld.nl/beveiliging/37249-dataportabiliteit-sluit-je-bij-ons-aan-of-verlies>> accessed 21 May 2016.

¹⁶ Chris Saad, ‘The data portability landscape – An update’ (The Data Portability Project, 18 December 2008) <<http://blog.dataportability.org/2008/12/18/the-data-portability-landscape-an-update/>> accessed 14 May 2016.

¹⁷ European Data Protection Supervisor, ‘Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy’ (Preliminary Opinion) (March 2014) 15 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf> accessed 21 May 2016.

¹⁸ *ibid.*

¹⁹ Directive 2002/22/EC on universal services and users’ rights relating to electronic communications networks and services (Universal Service Directive) (2002) OJ L108/51, art 30.

²⁰ Saad (n 16).

²¹ Eleni Kamateri, Nikolaos Loutas and others ‘Cloud 4SOA: A Semantic-Interoperability PaaS Solution for Multi-cloud Platform Management and Portability’ in Kung-Kiu Lau, Winfried Lamersdorf and Ernesto Pimentel (eds), *Service oriented and cloud computing* (Springer 2013) 66.

²² *ibid.*

²³ Saad (n 16).

²⁴ David De Vleeschauwer, ‘Dataportabiliteit bij sociale netwerksites: afdwingbaarheid onder privacywetgeving, mededingingsrecht en consumentenrecht’ (Master thesis, KU Leuven 2012–2013) 4.

²⁵ Kamateri, Loutas and others (n 21) 66.

²⁶ This argument is notably used by the European Commission to plead in favour of data portability and is discussed in [section 3.2](#) of this contribution.

competition.²⁷ Therefore, allowing personal information to be transferred without hindrance would counterbalance the lock-in of the user into one service.

Besides the advantages for the users, data portability also grants advantages to the service providers. According to Elias Bizannes, chairperson and executive director of the Data Portability Project, "site owners have an economic interest to support the portability of people's data".²⁸ He believes that allowing users to transfer their data easily and in a transparent manner will increase the feeling of the customers to feel free to move and drive them to share their personal information more easily than before.²⁹ If personal data became portable, service providers could benefit from it by collecting information they did not have before. This will additionally be beneficial for targeted advertising, providing service providers with up to date information on their consumers.³⁰ Moreover, Elias Bizannes believes that there exists a relationship between sites and their users. Data portability would increase the trust existing between the two and therefore have a positive effect on the users' online experience.³¹ As users would become more aware of how their data is being used, the sites offering the most transparency will be the "chosen ones".

2.3.2. *The drawbacks of data portability*

Attributing online users the right to transfer their personal data between different online services without hindrance raises controversy.

The major concern about data portability is the potentially adverse effect on privacy.³² Research has shown that the main preoccupations of experts in the field of privacy and social network application are associated with the inability of users to keep control over the transfer of their personal data and the lack of transparency of the process.³³ Indeed, a disadvantage of data portability is that it increases the complexity of control and process of personal data.³⁴ The procedures are often not clear to the users and only minimal privacy settings are in place, which are not sufficient to protect effectively the user's privacy.³⁵ Therefore, the Data Portability Workgroup has been criticised by scholars who deplore the lack of privacy safeguards for the users.³⁶

Additionally, companies that are part of the Data Portability Project are not entirely convinced by the concept itself. In fact, the former Chief Privacy Officer (CPO) of Facebook

explained his point of view regarding data portability in an interview in 2008.³⁷ During this interview, he explained that although Facebook is serious in engaging in data portability discussions, they fear privacy and security issues.³⁸ Data portability would, according to the former CPO of Facebook, constitute an open door for companies who would exploit personal data and take more than what is necessary for the service they are offering.³⁹ Therefore, Facebook wants to assure that their users' data is safe by creating adequate rules and controls.⁴⁰ In other words, Facebook does not seem to allow a complete portability of its users' data and is reluctant to make it interoperable with other systems.

Another concern resulting from data portability is related to the consequences in case of identity fraud. Truly, the repercussions would be more important when the transfer of personal data is facilitated, impairing the privacy of the owner of the data.⁴¹ Furthermore, users of those online services are often not realising the existing risks to the privacy of their information.⁴²

A third issue concerns the intellectual property risk. Knowing who owns data and to which extent data is considered personal data. Facebook provides a good example as a user's Facebook profile is constituted of friends' lists, pictures that are taken by the user or on which he is tagged, and videos he has posted and so on. It is questionable whether a user should be allowed to transfer all this information on another site. Indeed, it is his personal choice and indeed, it is the result of years of posting. However, should it be admitted to take your friends list to other services and therefore give your friends data to services without this friend's consent? The same question could be asked for pictures. How should we deal with pictures being transferred from one site to another? A person that is on this picture has no more control on the information that is circulating on the Internet anymore. A last example concerns the videos that are posted. In most of the cases, these are coming from YouTube. Therefore, intellectual property issues might appear, as these videos are not personal data of the online user but just part of their profile history. This is a much-discussed topic, which presented a hurdle for the European Commission when considering the questions of data portability.

Finally, a significant theme should be discussed when considering data portability. Potential issues arise for many companies who have their business model based on the processing of personal data that are given by their users in order to offer a service. An example could be an Online Fashion Advisor. This site would prepare number of personal questions related to the tastes of its users, their leisure activities, etc., process this information and offer the best combination

²⁷ Laise Bornico and Ian Walden, 'Ensuring competition in the clouds: the role of competition law?' (2011) 12(2) ERA Forum 265, 282.

²⁸ Elias Bizannes, 'Why Every Site Should Have Data Portability Policy' (Techcrunch, 23 June 2010) <<http://techcrunch.com/2010/06/23/data-portability-policy/>> accessed 21 May 2016.

²⁹ *ibid.*

³⁰ *ibid.*

³¹ *ibid.*

³² Christopher S. Yoo, 'When Antitrust met Facebook' (2012) 19 George Mason Law Review 1147, 1155.

³³ Stefan Weiss, 'Privacy threat model for data portability in social networks applications', (2009) 29 International Journal of Information Management 249, 250.

³⁴ *ibid.*

³⁵ *ibid.*

³⁶ *ibid.*

³⁷ Juan Carlos Perez, 'Facebook privacy chief: Data portability dangers overlooked. Facebook's chief privacy officer acknowledges that there's more work to be done regarding the site's privacy concerns' (IDG News Service, 11 February 2008) <http://www.pcworld.idg.com.au/article/205551/facebook_privacy_chief_data_portability_dangers_overlooked/> accessed 21 May 2016.

³⁸ Perez (n 37).

³⁹ *ibid.*

⁴⁰ *ibid.*

⁴¹ Weiss (n 33) 250.

⁴² *ibid.*

of clothes for its customers. This is a business process that is entirely based on personal data of users. Therefore, with data portability, users would be allowed to transfer this profile, to a bigger competing online retail clothing store, which would use this information to recommend its own perfect outfits. The consequence being that the investments made by the Fashion start-up would be lost, as they would lose the majority of their customers over bigger firms. One could therefore argue that the incentive for companies to start a new concept based on the processing of information in order to offer a service would be lowered if the right to data portability were enforced. Although the problem is not similar, the same arguments could be used against making Facebook's data portable. Although the information is entirely given by its users, the way they are processed and put into place is entirely made by Facebook, which costs time, energy and people. It is therefore maybe unreasonable to allow the portability of all personal data without hindrance.

3. Enforcing data portability under European Competition Law?

3.1. Overview

In some circumstances, the restriction to data portability can be sanctioned by European Competition Law if it qualifies as an abuse of a dominant position as mentioned in article 102 of the TFEU.⁴³ In 2012, the former Commissioner for Competition Policy, Joaquín Almunia, recognised the lock-in problem due to services restricting the portability of data of their users.⁴⁴ In the same context, the Commissioner recognised the necessity for users to transfer their data or personal content without switching barriers in order to obtain a healthy competition environment.⁴⁵ To attain this aim, he affirmed that the General Data Protection Regulation would be favourable but did not exclude the possibility for EU competition law to apply.⁴⁶ For this reason, it can be assumed that the European Commission can take action against dominant firms who constrain their users to transfer their data to another service, based on European Competition Law.⁴⁷

Because the application of competition law is a presumed tool to attain data portability, this part will analyse its possible application. In this regard, it will be first analysed when article 102 of the TFEU can be applied to data portability and to whom.

3.2. The application of European Competition Law to data portability

Limitation on data portability may be sanctioned by European Competition Law under article 102 of the TFEU. This article aims at prohibiting dominant undertakings behaving in an abusive way and is only applicable to dominant undertakings. Therefore, an analysis will first have to be done on when an undertaking is dominant and what the relevant market is in the context of online services. Once an enterprise is considered dominant, an abusive behaviour has to be shown. In this context, under certain circumstances limitation to data portability can be considered an exclusionary practice, which can constitute an abusive behaviour. Regarding those different conditions necessary in order to appreciate when competition law can be applicable to data portability, an analysis of these key terms appears to be necessary.

3.2.1. Assessment of the dominant market power

The first step when assessing the application of article 102 TFEU is to evaluate whether an undertaking has dominant market power.⁴⁸ The European Court of Justice (ECJ) has defined 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”.⁴⁹

Generally, the European Commission evaluates the dominant position of an undertaking by making an assessment of market shares,⁵⁰ which are an indicator of the importance of different undertakings that are active on the market.⁵¹ Thereby, they consider that firms that have fewer than 40% of market shares will be very unlikely to have a dominant position in the market. Furthermore, the ECJ case law reveals that market shares of 50% or more are in principal a clear evidence of the existence of market power.⁵² However, in certain markets such as the one applying to social networking providers, high market shares are not necessarily indicative of market shares.⁵³ However, in European Competition law, unlike under US anti-trust law,⁵⁴ no other criteria exist yet for this particular area.

⁴⁸ Commission, ‘Guidance on the Commission’s enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings’ (Communication) C45 (2009) 02.

⁴⁹ Case C-27/76 *United Brands v Commission* (1978) ECR 207, para 65.

⁵⁰ Commission (n 48).

⁵¹ European Data Protection Supervisor, ‘Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy’ (Preliminary Opinion) (March 2014) 6 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf> accessed 07 May 2016.

⁵² See cases: Case C-85/76 *Hoffman-La Roche v Commission* (1979) ECR 461, para 41 and Case C-62/86 *Akzo Chemie v Commission* (1991) ECR I-3359, para 60.

⁵³ De Graef, Verschakelen and Valcke (n 47) 59.

⁵⁴ Notably through the “network effect” which will be examined in section 6.3.1 of this paper.

⁴³ Bornico and Walden, (n 27) 282.

⁴⁴ Commissioner Almunia, ‘Competition and Personal Data Protection’ (Privacy Platform Event: Competition and Privacy in markets of Data, Brussels, 26 November 2012), <http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> Accessed 21 May 2016.

⁴⁵ Commissioner Almunia (n 44).

⁴⁶ *ibid*.

⁴⁷ Inge De Graef, Jeroen Verschakelen and Peggy Valcke, ‘Putting the right to data portability into a competition law perspective’, (2013) Annual review, *The Journal of the Higher School of Economics* 53, 58.

3.2.2. *The relevant market for online services*

Defining the relevant market is necessary in order to determine the scope of a dominant position.⁵⁵ The European Commission uses a method in order to define the relevant market on a case-to-case basis.⁵⁶ When assessing the relevant market, the European Commission starts with examining if products or services belong to the same market.⁵⁷ Therefore, the substitutability criterion is used. This criterion examines if a service can be replaced by a similar service. Applying this to online services is rather complicated when considering the number of online services offered. Indeed, online services go from search engines, to online shopping, social networking or price comparison sites. These online services have created new products, which are constantly evolving and partly interacting with one another. Given the high concentration of the online environment, it is very difficult to determine the relevant market for online services. This results in a difficulty in measuring a company's market share and then demonstrating that a company has a dominant market power.⁵⁸

3.2.3. *Assessment of an exclusionary conduct*

Once it has been shown that an undertaking has a dominant position in the relevant market, the European Commission has to verify if this undertaking acts in an abusive manner. This second step in the assessment of the applicability of article 102 of the TFEU is evaluating the existence of a so-called "exclusionary conduct".

Exclusionary conduct can be defined as a situation in which "a dominant undertaking excludes actual or potential competitors by means other than competing on the merits of the products or services they provide".⁵⁹ The latter is abusive where the conduct of the dominant undertaking is foreclosing competitors in an anti-competitive way.⁶⁰

In the context of data portability, by restricting their users from transferring their data to another service, online service providers are acting in a way that could be considered as anti-competitive.⁶¹ Those restrictions create switching costs, which result in a lock-in of the user and have negative

consequences on new entrants.⁶² Restrictions on data portability have great repercussions in markets where the network effect is prominent. Indeed, in those markets, restrictions on data portability may be used strategically by firms in order to acquire a dominant position and to maintain it for a long period.⁶³

According to Peter Swire and Yianni Lagos, restrictions on interoperability or the failure to write an export-import Module constitute an exclusionary conduct.⁶⁴ In fact, they believe this behaviour can be interpreted by Competition law in three different ways.

The first form of exclusionary conduct is the so-called 'refusal to supply'. This concept originates from U.S. Anti-trust law's "refusal to deal" theory.⁶⁵ In European Competition law, the European Commission applies this theory to exceptional circumstances. They consider that generally speaking, an undertaking should "have the right to choose its trading partners and to dispose freely of its property".⁶⁶ In this regard, they will consider the behaviour of a firm as anti-competitive only when it falls under three conditions: "the refusal relates to a product or service that is objectively necessary to be able to compete effectively on a downstream market, the refusal is likely to lead to the elimination of the effective competition on the downstream market, and the refusal is likely to lead to consumer harm".⁶⁷ Subsequently, if a dominant undertaking refuses or restricts transfer of personal data that is considered 'indispensable' and if this refusal harms effective competition as well as consumers, it will be considered as an exclusionary conduct.⁶⁸ Consequently, article 102 TFEU could apply.

The second form of exclusionary conduct is the essential facilities doctrine. The latter is very close to the theory of refusal to supply. This doctrine makes an exception to the freedom of a company to choose with whom it deals, when a monopolist undertaking refuses to administer inputs that are essential to competition even though doing so is feasible.⁶⁹ The difference with the 'refusal to supply' doctrine resides in the fact that the latter applies to situations where a previous relationship exists between the dominant firm and its competitors, whereas the essential facilities doctrine concerns a situation in which a firm wants to enter a new market in order to broaden its power and refuses to share with new competitors.⁷⁰

The question is whether personal data could be considered as an "essential facility". There is no clear answer yet, but both the European Commission and the EU Courts consider that a firm refusing to give access to an essential input may

⁵⁵ Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (20013) OJ L001/001.

⁵⁶ Commission Notice on the definition of relevant market for the purposes of Community competition law (1997) OJ C372/0005.

⁵⁷ *ibid.*

⁵⁸ For more information regarding the relevant market, please refer to the paper of Paul T. Moura, 'The sticky Case of Sticky Data: An examination of the Rationale, Legality, and Implementation of a Right to Data Portability Under European Competition Law' (2014) Media@LSE Electronic MSc Dissertation Series <<http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/MScDissertationSeries/2013/118-Moura.pdf>> accessed 21 May 2016.

⁵⁹ European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (Preliminary Opinion) (March 2014)6<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf> accessed 06 February 2016.

⁶⁰ Commission (n 48) 2 §19.

⁶¹ Bornico and Walden (n 27) 275.

⁶² *ibid.*

⁶³ *ibid.*

⁶⁴ Peter Swire and Yves Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', 72(2) *Maryland Law Review* 335(2013), 360.

⁶⁵ *ibid.* 361.

⁶⁶ Commission (n 48) 75.

⁶⁷ Commission (n 48) 81.

⁶⁸ Swire and Lagos (n 64) 362.

⁶⁹ Zachary Abrahamson, 'Essential Data' (2014) 124(3) *Yale Law Journal* 867.

⁷⁰ Ali A. Massadeh, 'The Essential Facilities Doctrine Under Scrutiny: EU and US Perspective' (2011) UEA Law School Working Paper Series <<http://ssrn.com/abstract=1738326>> accessed 20 February 2016.

breach article 102 TFEU if three conditions are fulfilled.⁷¹ Therefore, an online service provider would have to make the personal data it has of its user interoperable under competition law if it is a dominant firm, if the data is essential or indispensable for its rivals to carry out their business on a downstream market and if not making data interoperable harms the consumer.⁷²

Finally, the third way in which restrictions to data portability could be interpreted is through the concept of tying.⁷³ Peter Swire and Yianni Lagos put forward the hypothesis that by creating a software program that is not interoperable, social networks might be tying their products, before taking down this assumption.⁷⁴ In order to prove tying, the European Commission uses three conditions. First, the behaviour has to be taken by a dominant undertaking in the tying market. Second, the tying and tied products have to be distinct and finally the tying practice has to lead to an anti-competitive foreclosure.⁷⁵ When going through those conditions, we realise that it is a rather complicated task to apply the tying concept to restrictions to data portability. First, the dominant position of an online provider is hard to demonstrate. Secondly, a software and its Export–import Module are not two separate products.⁷⁶ In this regard, I believe the tying doctrine would not be applied to a data portability case.

4. Conclusion

The analysis whether European Competition Law could be applied to data portability cases raises some difficulties. It cannot be excluded that article 102 of the TFEU may apply to some anti-competitive situations resulting from restrictions on data portability. Nevertheless, it appears to be challenging to apply European Competition Law to data portability. Its enforcement requires indeed the fulfilment of a number of conditions, which are hard to apply to online services.

As it is challenging to apply European Competition Law to data portability cases, the next section will analyse whether U.S. antitrust law can be a source of inspiration for the European Legislators when considering data portability in the context of European Competition Law.

5. Monopolisation claims for restricting data portability: U.S. antitrust law

5.1. Overview

The discussions held about data portability in the United States are diverging from those in Europe. The main difference is that

this issue is addressed through the application of antitrust laws rather than privacy legislation.⁷⁷ Therefore, emerging online service providers could win monopoly claims if they prove that their competitors are violating antitrust law by not providing or supporting data portability tools.⁷⁸ Nevertheless, the sphere of online services causes several potential issues when applying antitrust law. The conditions usually used in order to assess monopoly power are not easily applicable to this sector, which causes difficulties when trying to prove the latter in an online context.

In order to capture the problem, it is important to set up the U.S. antitrust frame. Therefore, the applicable legislation is first identified in this contribution. Afterwards, the conditions requested for antitrust legislation to apply are named and their application in the online sector is defined. This will lead to the discussion of some issues following the application of antitrust law to data portability issues. Once the latter is defined, the contribution focuses on U.S. case law in order to understand how the Courts address the matter. Finally, a reflection on what to expect for the future of interoperability through the application of antitrust law in the United States is made.

This part of the contribution refers mostly to examples related to social networking services as interoperability is highly discussed in this regard.

5.2. Applicable legislation

Unlike in European Competition law, U.S. antitrust law does not only prohibit the unilateral misuse of market power by monopolisation but also prohibits the attempt of monopolisation. The main applicable legislation is the Sherman Act.⁷⁹ Section 1 prohibits contracts, combinations of contracts and conspiracies in restraint of trade.⁸⁰ Section 2 is more relevant for our purposes as it prohibits the unilateral misuse of market power in order to monopolise or attempt monopolisation.

Furthermore, the Sherman Act is supported by a plethora of additional statutes and common law doctrines. The Federal Trade Commission Act is the most significant of those acts. It prohibits unfair competition methods.⁸¹ Its interpretation covers both “actual and incipient violations of the Sherman Act as well as anti-competitive conduct which violates the spirit of the antitrust laws”.⁸²

Another important act is the Clayton Act, whose Section 7 prohibits mergers and acquisitions that would have the effect of diminishing competition or creating a monopoly.⁸³

⁷¹ Geradin & Kuschewsky (n 2) 13–14.

⁷² *ibid.*

⁷³ Swire and Lagos (n 64) 363.

⁷⁴ *ibid.*

⁷⁵ Commission (n 48) 50.

⁷⁶ Swire and Lagos (n 64) 363.

⁷⁷ Barbara Sandfuchs, ‘Exclusionary Conduct and the Proposed Right to Data Portability’ (*Comparative Competition Blog*, 16 May 2014) <<http://comparativecompetition.blog.com/2014/05/16/exclusionary-conduct/>> accessed 3 May 2015.

⁷⁸ Sandfuchs (n 77).

⁷⁹ The Sherman Act Antitrust Law, Act of July 2, 1890 (26 Stat. 209).

⁸⁰ The Sherman Act, 15 U.S.C. para 1.

⁸¹ Federal Trade Commission Act, 15 U.S.C. paras 41–58, as amended.

⁸² Weber Waller, ‘Antitrust and Social Networking’ (2012) 90 North Carolina Law Review 1, 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1948690> accessed 21 May 2016.

⁸³ The Clayton Act, Section 7 15 U.S.C. para 18.

5.3. Requested conditions for antitrust law to apply

According to Section 2 of the Sherman Act, two conditions have to be fulfilled for antitrust law to be applicable.⁸⁴ First, it is required to prove that the competitor holds monopoly power. Then, only if this can be demonstrated the second requirement will apply. The second obligation is to prove that the firm, which has monopoly power, is engaged in exclusionary conduct.

Although the terms used are different, U.S. antitrust law and European Competition Law are relatively similar in the regard of their requirements. Indeed, article 102 of the TFEU prohibits similarly companies holding a dominant position that engage in abusive behaviour. Therefore, companies in Europe also have to possess a dominant position and abuse of this dominant position in order to be prohibited by European Competition Law. Nevertheless, regardless of those similarities, both legislations differ in various ways. Firstly, Section 2 of the Sherman acts applies both to monopolisation as well as to “attempted monopolisation”, whereas in European Competition law, only effective abuse of a dominant position can be prohibited. Secondly, there are some differences concerning the interpretation of the requirements, which will be discussed in the sections hereafter.

5.3.1. Possessing monopoly power

Comparably with European Competition Law, where companies have to hold a dominant position, U.S. antitrust law imposes the presence of monopoly power as a first condition. A distinction has to be made between firms that possess monopoly power and those that attempt to possess monopoly power. For the first ones, the possession of monopoly power will be a key element,⁸⁵ whereas for the second the dangerous probability of obtaining monopoly power, the specific intent to monopolise as well as an exclusionary conduct will be the key elements in order to prove attempted monopolisation.⁸⁶

It is important to point out that the mere possession of monopoly power is not regarded as illegal by antitrust law if it is the product of superior skills, foresight or industry.⁸⁷ This can be explained by the necessity to keep the incentive for firms to invest in innovative and valuable products or processes that are positive for economic growth.⁸⁸ However, antitrust law will prohibit acquired or maintained monopoly power through anticompetitive conduct.⁸⁹ In other words, a firm cannot be held liable for monopolisation or attempted monopolisation without owning monopoly power.⁹⁰

Before determining monopoly power itself, it is important to make a distinction between monopoly power and market power, which are related but not the same.⁹¹ The Supreme Court of the United States has defined both terms. Market power is

“the ability to raise prices above those that would be charged in a competitive market”⁹² whereas monopoly power is defined as “the power to control prices or exclude competition”.⁹³ In other words, monopoly power can be considered as a substantial market power. Similarly, several Court cases stated that “the evaluation of market power includes the examination of market share, but market share alone is insufficient to establish market power”.⁹⁴

Monopoly power is usually ascertained by measuring the market shares of a company in one or more relevant product and geographic markets.⁹⁵ The relevant market has been identified by different court cases as “the group of actual and potential producers of a product or service that consumers would view as reasonable effective substitutes. Such power can be shown by actual effects in the market place”.⁹⁶

According to U.S. Courts, firms need to possess dominant market shares.⁹⁷ Nevertheless, they have not yet identified a precise level at which monopoly power would be deducted.⁹⁸ The discussion about the requested market share in order to have monopoly power started in 1945 in the case *United States v. Aluminum Co. of America*.⁹⁹ In this case, it was stated that “a market share of ninety percent is enough to constitute a monopoly; it is doubtful whether sixty or sixty-four percent would be enough; and certainly thirty-three percent is not”.¹⁰⁰ This statement was followed one year later in the case *American Tobacco Co. v. United States*.¹⁰¹ Later, the Fifth Circuit Court stated that “monopoly power is rarely found when the defendant’s share of the relevant market is below 70%”.¹⁰²

In the European Union, the level of market shares requested to infer monopoly power is lower. Indeed, the European Court of Justice stated that unless the contrary is not proven, dominance can be presumed if an undertaking possesses persistently a market share above fifty percent.¹⁰³ Furthermore, the Office of Fair Trading considers that an undertaking owning less than forty percent of shares in the relevant market will be unlikely to be individually dominant unless other relevant

⁹² *NCAA v. Bd. of Regents of the University of Oklahoma* (1984) 468 U.S. 85, 109 note 38; see also *Jefferson Parish Hosp. Dist. No. 2 v. Hyde* (1984) 466 U.S. 2, 27 note 46.

⁹³ *United States v. E. I. du Pont de Nemours & Co. (Cellophane)* (1956), 351 U.S. 377, 391.

⁹⁴ *Bacchus Indus., Inc. v. Arvin Indus., Inc.* (1991) 10th Cir. Court 939 F.2d 887, 894; *Reazin v. Blue Cross & Blue Shield* (1990) 10th District Court 899 F.2d 951, 967; *Walter Bright and Ilene Bright, d/b/a Ace Ambulance Service v. Moss Ambulance Service, Inc., a Utah corporation, d/b/a Mountainwest Ambulance Service* (1987) 10th Cir. Court 824 F.2d 819, 824.

⁹⁵ *Weber Waller* (n 82) 4.

⁹⁶ *Weber Waller* (n 82) 4; *Brown Shoe Co. v. United States* (1962) 370 U.S. 194; *United States v. E.I. DuPont de Nemours & Co.* (1956) 351 U.S. 377.

⁹⁷ U.S. Department of Justice (n 172) 21.

⁹⁸ U.S. Department of Justice (n 172) 21.

⁹⁹ *United States v. Aluminum co. of America et al* (1945) 2d Cir. 144, U.S. 148 F.2d 416, 424.

¹⁰⁰ *United States v. Aluminum co. of America et al* (1945) 2d Cir. 144, U.S. 148 F.2d 416, 424.

¹⁰¹ *American Tobacco Co. v. United States* (1946) 328 U.S. 781, 813–814.

¹⁰² *Exxon Corp. v. Berwick Bay Real estate Partners* (1984) 5th Circ. 748 F.2d 937, 940.

¹⁰³ *Case C62/86 AKZO Chemie BV v Commission* (1991) ECR I-3359.

⁸⁴ See the Sherman Act, section 2.

⁸⁵ *United States v. Grinnell Corp* (1966) 384 U.S. 563, 570–571.

⁸⁶ *Spectrum Sports Inc. v. McQuillan* (1993) 506 U.S. 447, 459.

⁸⁷ U.S. Department of Justice, ‘Competition and single-firm conduct under section 2 of the Sherman Act: Chapter 2’ (*The United States Department of Justice*, 25 June 2015) 20 <http://www.justice.gov/atr/public/reports/236681_chapter2.pdf> accessed 21 May 2016.

⁸⁸ *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP* (2004) 544 U.S. 398, 407–408.

⁸⁹ U.S. Department of Justice (n 172) 20.

⁹⁰ *Weber Waller* (n 82) 4.

⁹¹ U.S. Department of Justice (n 172) 19–20.

factors provide strong evidence of dominance such as the weak position of competitors in the same relevant market or high entry barriers.¹⁰⁴

Although an accurate amount of owned market shares in the relevant market has not been defined in U.S. antitrust law and that holding high shares of the relevant market does not necessarily lead to monopoly power, it is still one of the most important factors when examining whether a firm has monopoly power or has a dangerous probability of obtaining monopoly power.¹⁰⁵ Nevertheless, it is very hard to calculate and demonstrate market share in the sphere of online services and notably within the sphere of social networking sites. Therefore, the second requirement will be more relevant for determining monopoly power of an online service provider.

As mentioned above, monopoly power is usually demonstrated when it can be shown that the firm has a high share of the relevant market and that there are entry barriers, either created by the firm itself or not.¹⁰⁶ Entry barriers are an indicator of true market power.¹⁰⁷ Indeed, a company possessing high market share in a market with low entry barriers may not indicate its ability to raise prices. On the other side, a company owning a high amount of market shares in a market with high entry barriers will indicate the possession of power of the firm and its ability to harm competition and consumers.¹⁰⁸ However, in the sector of online services, the question of barriers to entry and exit is not an easy one, especially in the social networking space. The technology and capital needed to create a social network are available and do not appear to have high barriers of entry. Nevertheless, other barriers exist to the creation of social networking sites, which constitute a sign of market power. The first one is the so-called “concept of network effects” and the second one is the “stickiness of the service”.

Normal rules are not applicable to social networks, as the costs for entering the market are minimal¹⁰⁹ and the technology needed is relatively restricted. Therefore, the alternative criterion of the “network effect” is used in the United States.¹¹⁰ When the value of a network is dependent of the number of users connected to it, there is a network effect.¹¹¹ Network effects can take two forms: they can be direct and indirect.¹¹² On the one hand, direct network effects are networks whose value directly increases as the numbers of users increase.¹¹³ On the other hand, indirect network effects “refer to systems where the development of complements increases the value of the system to users”.¹¹⁴ For instance, game consoles and their games could illustrate an indirect network effect. Similarly, DVD-players and disc would be an example thereof as well.

Both direct and indirect network effects apply to social networks. Indeed, the success of a social networking site depends greatly on the number of users, which make it more popular and valuable.¹¹⁵ Some may argue that although users have a high number of online friends, they usually only regularly interact with a limited number of those, thereby rejecting the network effect.¹¹⁶ This is a misconception of the network effect, which does not focus on the effective number of people we are connecting with while using a service, but with the possibility to connect and interact with a significant number of people. Therefore, “the more people that an individual subscriber can reach through the network, the more valuable the network becomes”.¹¹⁷ Furthermore, a social networking site offering more service than the traditional networking such as videos, calls or messaging, falls into the indirect networking effect.¹¹⁸

Another criterion that could be used to measure barriers to entry and exits in the scope of online service provider is the “stickiness of the system”. This term refers to the difficulty for users of a service to leave it, which reinforces the position of a company. A typical example is Facebook where it is indeed very difficult for Facebook users to leave their account. The stickiness of Facebook is mainly related to its social character. Indeed, as it is a platform on which people connect, exchange information and experiences. For this reason, having an account is crucial in order to keep connected, receive information or be aware of current events.¹¹⁹ This is true in different social circles such as private, professional or even political groups. Terminating a Facebook account is therefore very difficult because of its effect on your social life. It is also very well known that it can be perceived as abnormal to delete your account. This would alert your friends or family, which would be asking offline, if everything was fine.¹²⁰ Furthermore, it is technically not so easy to delete your account. Indeed, a time period of two weeks is required in order to take away all the users information, which remains Facebook’s property.¹²¹

The costs to switch to another service are another consequence of the “stickiness of a service”. As mentioned before in the chapter concerning European Competition Law, several sites such as clouds or online auction sites, make it very hard to switch to another similar service. This problem exists as well in the sector of social networking sites. Numerous social networking sites exist; nevertheless, it is very hard to move from one to another. The main reason is that social networking sites do not allow users to transfer their information from one site to the other. One would therefore have to start all over again, making a profile and downloading pictures, groups of interests, etc. if they choose to go to another social networking site. Over the years, some progresses were made in this regard. Since 2006, Facebook allows its users to share their Facebook information with third party websites.¹²² Nevertheless, it seems that it is more a possibility to import your information from

¹⁰⁴ Office of Fair Trading, “Assessment of market power. Understanding competition law”, (Competition Law guideline) 1, 7 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/1415.pdf> accessed 21 May 2016.

¹⁰⁵ U.S. Department of Justice (n 172) 23.

¹⁰⁶ U.S. Department of Justice (n 172) 23.

¹⁰⁷ Weber Waller (n 82) 15.

¹⁰⁸ *ibid.*

¹⁰⁹ *ibid.*

¹¹⁰ Yoo (n 32) 1148.

¹¹¹ Yoo (n 32) 1148.

¹¹² Weber Waller (n 82) 16.

¹¹³ *ibid.*

¹¹⁴ *ibid.*

¹¹⁵ *ibid.* 17.

¹¹⁶ Sandfuchs (n 77).

¹¹⁷ Yoo (n 32) 1148.

¹¹⁸ Weber Waller (n 82) 17.

¹¹⁹ *ibid.*

¹²⁰ *ibid.*

¹²¹ *ibid.*

¹²² *ibid.* 18.

third party service providers, to your Facebook account than the other way round.¹²³ In other words, importation was facilitated but exportation was not possible. Four years later, in 2010, Facebook allowed its users to download all the information they have into a ZIP file.¹²⁴ Although it provides its users the possibility to have a copy of this data, it cannot be used for another purpose than reading. The format in which the data is copied makes it incompatible for further use.¹²⁵

Until now, Facebook has not conferred further rights of portability of their user's data. This is also the case in other spheres of the online service providers' market.

In the end, proving the existence of barriers to entry and exit is difficult as the criteria normally applicable to examine this are not applicable to the online sphere. Nevertheless, as discussed above, other situations could be a sign of the existence of barriers to entry or exit, namely the network effect and the stickiness of the services' system. Even though they seem more appropriate, it is still being broadly discussed whether these could be used to assess the latter. The situations described here above such as the high number of users registered into a service, the difficulty to leave this service as well as to transfer your information to a new similar services, are signs of a company locking their customers into their service, which can be a sign of market power. This theory has been very strongly discussed.¹²⁶ It seems finally, that the applicability of these criteria will depend on the context.¹²⁷

5.3.2. Exercising exclusionary conduct

Once the requirement of dominant position has been demonstrated, it has to be shown that an undertaking exercises an exclusionary conduct.

The absence of data portability could support the claim of an exclusionary conduct. However, previous case law suggests that antitrust claims in the domain of data portability restrictions are unlikely to prevail. Indeed, as a general rule, antitrust law does not impose a duty to cooperate with your competitors.¹²⁸ In fact, the District Court has held in the decision *United States v. Microsoft*¹²⁹ that a monopolist who develops a product that is incompatible with its rival's products does not violate antitrust laws. Indeed, in order to violate antitrust law, "the incompatible products must have an anti-competitive effect that outweighs any pro-competitive justification for the design".¹³⁰ This obligation is strict and only applicable in some rare cases. One of them is the *Aspen Skiing v. Aspen Highlands Skiing* case¹³¹ in which the refusal of an undertaking to cooperate has clearly anti-competitive motives.¹³²

Two other recent cases illustrate the presumable difficulty to prove exclusionary conduct based entirely on an online service provider not offering data portability tools.

5.3.2.1. LiveUniverse Inc v Myspace Inc. LiveUniverse is the operator of a social networking site called vidilife.com. The dispute arose when Myspace reconfigured its website in order to prevent the downloading of Vidilife videos on Myspace web pages, removed all references to Vidilife and even prevented its users to access LiveUniverse's site from the Myspace site. LiveUniverse filed an antitrust claim as a reaction against those measures taken by Myspace.

This claim was dismissed by the district court for failure to allege actionable exclusionary conduct.¹³³ It supported its decision on the following points. Firstly, it attested that a company has generally a right to choose with whom it wants to deal and if it wants to deal at all. Although the Court previously imposed a duty to deal in the case *Aspen Skiing v. Aspen Highlands Skiing*,¹³⁴ this is not applicable in this case. The reason being that LiveUniverse and Myspace were involved following the decision of their users to incorporate content from LiveUniverse into Myspace and that they were therefore never involved in a voluntary agreement.¹³⁵ Secondly, the district court held that LiveUniverse "had no right to free ride on the traffic that Myspace was attracting to its website".¹³⁶ Finally, LiveUniverse claimed that the change of MySpace's product design constituted an exclusionary conduct and invoked the Microsoft case. This reasoning was rejected by the district court and the 9th Circuit Court, which concluded that: "LiveUniverse does not explain how MySpace's actions on its own website can reduce consumers' choice or diminish the quality of their experience on other social networking websites, which is the relevant market".¹³⁷

5.3.2.2. Facebook, Inc v Power Ventures, Inc. Power.com is a site offering the possibility to their users to integrate all of their social networking contacts into one site. In order to provide this service, Power Ventures uses the login information of the Facebook users to scrape off Facebook's information and display it on their site, Power.com.¹³⁸ Facebook sued Power Ventures for collecting Facebook's information, claiming that it violated several state and federal statutes concerning notably Copyright and Competition Law.¹³⁹ In response, Power

¹²³ *ibid.*

¹²⁴ See the link: <<https://www.facebook.com/settings>> accessed 21 May 2016.

¹²⁵ Weber Waller (n 82) 19.

¹²⁶ *ibid.* 20.

¹²⁷ *ibid.*

¹²⁸ See *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP* (2004) 540 U.S. 398.

¹²⁹ See *United States v. Microsoft Corp.* (2001) D.C. Cir. 253 F.3d 34, 75.

¹³⁰ See *United States v. Microsoft Corp.* (2001) D.C. Cir. 253 F.3d 34, 75.

¹³¹ See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.* (1985) 472 U.S. 585.

¹³² Sandfuchs (n 77).

¹³³ Yoo (n 32) 1158.

¹³⁴ See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.* (1985) 472 U.S. 585.

¹³⁵ Yoo (n 32) 1158.

¹³⁶ *ibid.* 1159.

¹³⁷ Sandfuchs (n 77).

¹³⁸ *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-5780 JF (RS), 2009 WL 3429568, art 1 (N.D. Cal. Oct. 22, 2009)

¹³⁹ Those claims were: the violating of the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. para 1030 et 22 seq.; the direct and indirect copyright infringement violating the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. para 1201, et seq. Facebook also asserts claims for relief based on state and federal trademark law and under California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code para 17200, et seq.

Ventures counterclaimed that Facebook was engaging in exclusionary conduct by asking their users names and passwords of other service providers such as Gmail or Hotmail, in order to access them directly from Facebook while preventing its competitors from doing the same.¹⁴⁰ The district court dismissed their counterclaim arguing that the access granted to Facebook by third party websites did not oblige Facebook to grant them unrestricted access to their site.¹⁴¹ It is indeed precedent that a company does not violate antitrust laws by introducing a product that is not interoperable with competing products.¹⁴² The district court added that “if Facebook has the right to manage access to and use of its website, then there can be nothing uncompetitive about taking legal action to enforce that right”.¹⁴³

5.4. How effective are antitrust claims regarding online service providers refusing to cooperate?

The eventual success of antitrust claims for not supporting or providing portable tools appears to be restricted. Many barriers are present that make it hard to prove monopoly power as well as exclusionary conduct in the online services sphere.

When analysing the requirements for monopoly power, some difficulties can be recognised. Firstly, it is hard to demonstrate market power through the possession of market shares since it is difficult to determine the relevant market. Secondly, the normal conditions are not applicable to barriers to entry and exit. For instance, costs cannot be used as a criterion. Therefore, the network effect would be more appropriate. Nevertheless, it is still discussed whether it can be used as a criterion in antitrust cases.

Finally, it seems like the possible success of claims demonstrating an exclusionary conduct as part of an antitrust claim can be questioned when seeing the results of the LiveUniverse and Power Ventures cases. Indeed, actions such as social networks refusing to deal with competitors, the designing of websites that are incompatible with sites of competitors as well as the refusal to enable data portability seem unlikely to be considered as exclusionary conduct in the United States, which will make them consequently unlikely to support antitrust liability.¹⁴⁴ According to Steven Vachani, chief executive officer of Power Ventures, “Facebook has established a dangerous precedent for the future of users’ right to own and control their data”.¹⁴⁵

5.5. Reflection: Could U.S. antitrust law be a source of inspiration for European Institutions when defeating the vendor lock-in issue?

Although U.S. antitrust law seems more easily applicable as it does not only apply to monopolisation but also to attempted monopolisation, the application of U.S. antitrust law to defeat restrictions on data portability seems a hard task. The United States’ Courts tend to allow online service providers to act in a restrictive way, preventing their competitors to use their site as well as their users to transfer information. Furthermore, the market shares required in order to have a dominant market share are much higher than in the European Union. It appears after the analysis of both legislations, that a data portability case would have more chance to succeed in the European Union than it would in the United States.

However, the chance for European Competition Law to be applied to data portability restrictions appears to be reduced. Therefore, I do not believe it is the right way to attribute a right to data portability. Therefore, the following section will examine the application of the new General Data Protection Regulation in order to see whether the latter offers a better chance for data portability to be attributed.

6. Data portability and the general data protection regulation

6.1. Overview

Data portability was introduced in 2012 by the European Commission in its proposal for a General Data Protection Regulation,¹⁴⁶ which will be part of the new legal framework for the protection of personal data in the European Union.¹⁴⁷ Considering the importance of this matter, the EC integrated this right in a Regulation rather than a Directive and uses thereby the strongest way to increase harmonisation and coherence.¹⁴⁸

As a part of the European legislative process, the European Parliament and the Council of the European Union reviewed the proposal. In this context, the right to data portability has been through several modifications.¹⁴⁹ The latter

¹⁴⁰ Yoo (n 32) 1160.

¹⁴¹ *ibid.*

¹⁴² *Facebook, Inc. v Power Ventures, Inc.*, No. C 08–5780 JW, 2010 WL 3291750, art 1, 13–14.

¹⁴³ *Facebook, Inc. v Power Ventures, Inc.*, No. C 08–5780 JW, 2010 WL 3291750, art 1, art 14.

¹⁴⁴ Yoo (n 32) 1160.

¹⁴⁵ Phil Milford, ‘Facebook Wins Lawsuit Against Power Ventures Over Login Data’ (Bloomberg Business, 17 February 2012) < <http://www.bloomberg.com/news/articles/2012-02-17/facebook-wins-summary-judgment-ruling-in-power-ventures-case-1> >, viewed on 15.05.2015 > accessed 7 May 2016.

¹⁴⁶ Proposal for a General Data Protection Regulation, 11 final.

¹⁴⁷ Commission, ‘Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century’ COM (2012) 9 final.

¹⁴⁸ According to article 288 of the consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, (2012) OJ C 326/0001 (TFEU), a regulation has a general application and is therefore binding and directly applicable to all Member States. Consequently, the same rules will be applicable to all Member States.

¹⁴⁹ Indeed, the proposal for a General Data Protection Regulation has been through several modifications since the first draft published by the Commission on the 25th of January 2012. On the 12th of March 2014, the European Parliament made amendments to the proposal, changing several points, concerning the right to data portability as well. On the 15th of June 2015, the Council of the European Union sealed a general approach on the Commission’s proposal for a GDPR and in June 2015, the European Parliament and the Council of the European Union started the trilogue negotiations in order to reach a final agreement at the end of 2015.

is an expression of both the contrasting interpretation the European Bodies have of data portability as well as the difficulty of the scope this right should entail.

The Regulation was agreed in December 2015 and encompasses for the first time a right to data portability in its article 20.¹⁵⁰ This constitutes an ambitious achievement considering the advantages as well as the possible downfalls of the attribution of this right.¹⁵¹

A brief analysis of the aims the European Commission wants to achieve with this new Regulation as well as the evolution of data portability throughout the legislative procedure are examined in the following sections.

6.2. Aims of integrating data portability in the regulation

The reason for integrating data portability in the GDPR can be explained as a part of achieving three main objectives.

The first objective is to create trust in the online environment in order to encourage economic development in the online environment.¹⁵² In this regard, enabling data to be portable will ensure the control by individuals of their personal data, the protection of individual's data when processed by European and non-European data processors¹⁵³ and reinforce the accountability of those processing personal data. This should reassure the consumer and create thereby more trust in the online services.

The second objective of data portability is to reduce the lock-in of the consumers. In cloud computing, the lock-in is considered as one of the biggest challenges because of restrictions on portability of personal data.¹⁵⁴ Because clouds are incompatible, the costs of switching are higher. Cloud providers may use it as an advantage by preventing their customers to move to a competitor, but this is at the detriment of the users.¹⁵⁵ For this reason, it is important to ensure data portability and make the different clouds collaborate.¹⁵⁶ The EC noted that there is no explicit right existing that would enable an individual to extract his information in order to transfer it to another service or application.¹⁵⁷ Due to the lack of interoperability, new services that are cheaper, better or more privacy friendly for example, are confronted with the difficulty of attracting new users.¹⁵⁸ Certain online services are used so much that the amount of data collected is very important. This results in a fear of users to lose this data in the event of changing provider. Therefore, the European Commission stated: "This

situation effectively creates a lock-in with the specific service for the user and makes it effectively very costly or even impossible to change provider and benefit from better services available on the market. Portability is a key factor for effective competition, as evidenced in other market sectors, e.g. number portability in the Telecom sector".¹⁵⁹

Thirdly, in the line of fighting the lock-in effect, data portability would require online providers to share the user personal data they possess. This would consequently also reduce monopoly power and therefore improve competition in the market, enabling new entrants to attract new users.¹⁶⁰

Public authorities and citizens requested the European Commission to take action in order to create additional competition between Internet providers and thereby erase their dependency.¹⁶¹ The users asked for a right of informational self-determination. The latter is a concept that originates from the German Constitutional Court in 1983.¹⁶² In this decision, the Court ruled that an individual loses the freedom to make decisions based on his own self-determination if he cannot "survey with sufficient assurance the information concerning himself known in certain areas of his social surroundings, and whoever is not in a position to assess more or less the knowledge of possible partners in communication".¹⁶³ In other words, people would have a right to determine for themselves what they do with their personal information.

6.3. Evolution of data portability in the GDPR

The changes made to the proposal for a GDPR by the three European Legislative Bodies show that they do not interpret the right to data portability in the same manner.

The European Commission had the ambition to grant the right to data portability as a right on its own, in one article.¹⁶⁴ It regarded it as a right for the individual to obtain both a copy of its personal data that is being processed as well as a right to require the controller to transfer its personal data directly to another controller. This right is broad for the data subject as it concerns not only personal data of the subject, but also any other information. This demonstrates a will by the EC to grant an extensive right to data portability. It is furthermore clear that the benefits of the data subject are privileged, regardless of the burden that may be created on the part of the controllers and processors as the concerned data should be transferred without hindrance.¹⁶⁵

The European Parliament mainly follows the ideas of the European Commission as it grants the same rights, but as part

¹⁵⁰ GDPR, art 20.

¹⁵¹ See Section 2.3.2 of this contribution.

¹⁵² Proposal for a General Data Protection Regulation, recital 1.

¹⁵³ General Data Protection Regulation Impact assessment, recital 61.

¹⁵⁴ Meriem Thabet and Mahmoud Boufaïda, 'An Agent-Based Architecture and a Two-Phase Protocol for the Data Portability in Clouds' (27th International Conference on Advanced Information Networking and Applications Workshop, Barcelona, 25 March 2013).

¹⁵⁵ *ibid.*

¹⁵⁶ *ibid.*

¹⁵⁷ General Data Protection Regulation Impact assessment, recital 28.

¹⁵⁸ General Data Protection Regulation Impact assessment, recital 28.

¹⁵⁹ General Data Protection Regulation Impact assessment, recital 28.

¹⁶⁰ Swire and Lagos (n 64) 338.

¹⁶¹ General Data Protection Regulation Impact assessment, recital 28.

¹⁶² Bundesverfassungsgericht, Urteil vom 15.12.1983, BverfgGE 65, 1, 41 (more famous as the Census decision).

¹⁶³ Bundesverfassungsgericht, Urteil vom 15.12.1983, BverfgGE 65, 1, 41 (more famous as the Census decision).

¹⁶⁴ Notably in Article 18 of the proposal for a GDPR that was divided in three paragraphs.

¹⁶⁵ Swire and Lagos (n 64) 342.

of a general right to access.¹⁶⁶ Additionally, modifications were made to the scope of the concerned right. Firstly, the data concerned should be, according to the EP, only personal data of the data subject. Furthermore, it requires the copy to be given in an interoperable format, giving more precisions to the format that should be used to give the copy to the data subject. It also deleted the third paragraph of the original proposal, which left the power to the Commission to adopt implementing acts regarding data portability.¹⁶⁷

The Council of the European Union on the other hand, focuses more on the one hand on privacy and intellectual property rights and seems on the other hand to advantage the controllers and processors.¹⁶⁸ Indeed, by granting the right to data portability only with a copy and deleting the possibility to request a direct transfer of your information, one could argue they are trying to protect the data subject by avoiding its data to be transferred without their consent. On the other hand, it can be argued that interoperability would be too costly and difficult for the controllers and processors to implement. As what concerns the intellectual property right, the Council is clear in protecting this by refusing the transfer of a copy, if it infringes copyright law. Although this was presupposed in the proposal, it is now clearly written. Finally, the Council is very strict on the right to obtain a copy. Based on the above statements, one could argue the Council is not in favour of the data portability right and only wants to attribute this right in a minimal manner.

Because of this European legislative procedure, an agreement was reached and data portability is now integrated in article 20 of the GDPR, which refers to three rights.

Firstly, the GDPR recognises the right for the data subject to receive the personal data he has provided to a controller in a “structured, commonly used and machine-readable format”.¹⁶⁹

Secondly, the data subject has the right to transmit this data he received from the controller to another controller and this without hindrance.¹⁷⁰ This right is only given if the processing of the personal data fulfils two cumulative conditions. On

the one hand, the data has to be processed with the consent of the data subject and on the other, it has to be carried out by automated means.¹⁷¹

Finally, the data subject has the right to ask for his personal data to be transferred directly from one controller to the other, where it is technically feasible.¹⁷²

In my opinion, the last version of data portability as referred to in article 20 of the GDPR goes in favour of the data portability right. Some terms are however unclear regarding their interpretation. This is discussed in section 6 of this contribution.

7. Concerns regarding the proposal for a general data protection regulation

7.1. What type of data falls under the data portability right?

The right to data portability will have consequences on controllers or processors, which provide means for possessing personal data.¹⁷³ Therefore, it is crucial for them to understand which data falls under this right. The GDPR attributes the right for the data subject to make his personal data portable. Even though it is clearer than the original scope of data concerned which also included “any other information provided by the data subject”, personal data still leaves some room for interpretation.

Originally, personal data was defined in the proposal for a GDPR in its article 4(2) as “any information relating to a data subject”. Being a short and rather imprecise definition, it has been amended by the EP and was taken over into the GDPR in article 4(1). The GDPR defines personal data as follows:

*any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person.*¹⁷⁴

According to this definition, it seems clear that personal data inserted by the data subject, is considered personal data and benefits from the data portability right. Examples thereof can be personal information communicated by the individual when registering in an online service such as the name, the gender, the birth date or other personal information. Beside this type of information, data such as uploaded files, pictures or status updates should also be considered protected personal data.¹⁷⁵

Next to this type of information, providers also hold other type of data such as statistics about the use of their website, creating data used for analytical purposes.¹⁷⁶ Because this type

¹⁶⁶ European Parliament, ‘Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ COD (2012) 0011, article 15(2).

¹⁶⁷ Javier Huerta Bravo, ‘BITS seminar discusses data portability at the crossroads of data protection and competition policy’, (Cullen International, Brussels, 9 May 2014) 3 <<http://www.cullen-international.com/asset/?location=/content/assets/training--conferences/conferences/2014/flash---bits-seminar-discusses-data-portability-at-the-crossroads-of-data-protection-and-competition-policy.pdf/flash---bits-seminar-discusses-data-portability-at-the-crossroads-of-data-protection-and-competition-policy.pdf>> accessed 21 May 2016.

¹⁶⁸ See: Council of the European Union, ‘Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – preparation of a general approach’, (9398/15), article 15(1b) <<http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>> accessed 21 May 2016.

¹⁶⁹ General Data Protection Regulation, art 20, §1.

¹⁷⁰ *ibid.*

¹⁷¹ General Data Protection Regulation, art 20, §1, (a) (b).

¹⁷² General Data Protection Regulation, art 20, §2.

¹⁷³ Proposal for a General Data Protection Regulation, recital 15.

¹⁷⁴ General Data Protection Regulation, art 4(1).

¹⁷⁵ Swire and Lagos (n 64) 347.

¹⁷⁶ De Graef, Verschakelen and Valcke (n 47) 56.

of data is most likely to be the result of an aggregation of several data, it will not be possible to link this data back to the individual. For this reason, it is most probably not going to fall into the scope of the data portability right.¹⁷⁷

A line can be drawn quite easily between these two types of data, which makes it possible to know if it falls under the data portability right or not. Nevertheless, there is a third type of data, which lies in between this data and is processed by online service providers. The latter is a combination of information provided by the data subject as well as by the service provider. The question is whether this falls under the right to data portability and should be considered as “any information relating to an identified or identifiable natural person”. In this context, we will examine two examples.

A first illustration refers to the profile of sellers in an auction website. Websites such as eBay have created a system of reputation and feedback scores, which are of a great importance for the sellers. The portability of those profiles would be of great importance for new auction entrance but is this data covered by the right to data portability? Unfortunately, the European Commission did not define “any other information relating to an identified or identifiable person”.

I believe nevertheless, that this type of data should be portable and fall under the scope of personal data. Indeed, I regard that the information referring to a person’s reputation or feedback score is related to the data subject, even though this data was not given by the individual, and should therefore fall under the scope of data portability as “personal data”.

The second illustration is related to avatars created in online gaming sites such as World of Warcraft.¹⁷⁸ Users in this game create individualised avatars and the question is if those avatars can be presumed to constitute information related to the data subject. I believe this can be discussed. It is indeed information created by the players and the result of their work, time and imagination. On the other hand, the possibility to create an avatar and the choices of avatars are the creation of the game platform. Gamers will probably consider this as personal information whereas the controller will consider the opposite. If considered personal data, this would raise some new interoperability issues, imposing the service providers to have interoperable avatars. Regardless of the fact that the data subject created this type of data, I believe it is highly improbable that such type of data would be considered as personal data, covered by data portability. In reality, it is hard to argue in favour of this type of data being personal data that should be falling under the right to data portability. Every game has its own avatars, which are the creation of developers and the result of investments. Therefore, making these portable would reduce the incentive to create new gaming platforms as their virtual players could be transferred in only a few click to a competing game platform. Furthermore, one of the aims of data portability is to ensure that the data subject has trust in the online environment by having the right to transfer information that concerns him. I believe this could not be considered a motive strong enough to attain this goal. As the latter

constitutes a rather extreme example, it nevertheless shows the importance of defining the term “personal data” correctly.

Online services are numerous nowadays and the data flowing is very different and specific to certain services. Therefore, it is crucial that a definition thereof is provided. Furthermore, guidance from the European Institutions on how to handle with the nuanced issues concerning the information that is provided by both the data subject and the controller will be necessary to execute correctly the data portability right.¹⁷⁹

Jurisprudence of the Court of Justice of the European Union (CJEU) will be of great importance as well. A case regarding the interpretation of “personal data” as stated in article 2(a) of the EU Data Protection Directive 95/46/EC is currently ongoing.¹⁸⁰ In this case, the question has been raised whether dynamic IP addresses can be “personal data” under certain circumstances. As the interpretation of “personal data” is primordial for the application of the GDPR, it can be expected that similar cases will appear in the years following the applicability of the GDPR.

7.2. Territorial scope

Another concern is related to the territorial scope of the General Data Protection Regulation. The latter has an extended scope of applicability and affects controllers and processors that are based outside the EU and provide means for processing personal data in the European Union. Currently, under the Directive, European data protection law applies to controllers based outside the European Union if their equipment used to process data is located in the EU.¹⁸¹ Under the GDPR, all entities established outside the EU that either offer goods or services to EU residents or monitor the behaviour of EU residents will be subject to the Regulation.¹⁸² The consequences for non-EU entities that will be falling under the Regulation are significant, as they will have to appoint a representative for the European Union. The representative’s role is to “act on behalf of the controller and to be answerable to the EU data protection authority”.¹⁸³ On the other hand, the Regulation requires the appointment of a representative in only one Member State, whereas the Directive required the designation of a representative in each Member State where it uses “means of processing”.¹⁸⁴

¹⁷⁹ *ibid.*

¹⁸⁰ Case 582/14-Patrick Breyer v Germany <<http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN&cid=1095511>> accessed 28 May 2016.

¹⁸¹ X, ‘The Proposed EU General Data Protection Regulation-A guide for in-house lawyers’, (June 2015) Hunton & Williams 1, 10 <https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf> accessed 10 September 2015.

¹⁸² General Data Protection Regulation, art 3 (2).

¹⁸³ Patrick van Eecke, Cameron Craig and Jim Halpert, ‘The first insight into the European Commission Proposal for a new European Union data protection law’, (February 2012) 15.8 Journal of Internet Law 19, 20.

¹⁸⁴ X (n 181).

¹⁷⁷ Swire and Lagos (n 64) 347.

¹⁷⁸ Swire and Lagos (n 64) 348.

7.3. Interpretation of some key terms

7.3.1. The format

Article 20 of the General Data Protection Regulation states that the data controller has to provide the data subject's personal data in a structured, commonly used and machine-readable format.¹⁸⁵

A structured format would be a data format that “allow for increased functionality and easier data transfer”¹⁸⁶. Examples of structured formats would be RDL/XML, which enable an easier transfer of data.¹⁸⁷ PDF is for example not a structured format as it displays all the information as one image, making its further use difficult.¹⁸⁸ A structured format can however encompass machine- and human-readable data.¹⁸⁹ In its proposal for a GDPR, the European Commission originally intended to examine the formats used by the providers and determine whether they are in accordance with the requested format or not.¹⁹⁰ This was nevertheless amended and replaced by the requirement for the format to be machine-readable. The latter encompasses all formats, standard or not, that enable the further use of information as they can be read by a computer system or web browser and therefore enable an automatic processing of the data.¹⁹¹

In the amended version of the proposal, the European Parliament wanted to go beyond this requirement, choosing the format to be interoperable. This has the consequence that the format does not only have to be easily reusable but that it should also be compatible with other systems in order to make data from other origins processable.¹⁹² The latter would make the right to data portability stronger as it would make it easier to transfer the data. Nevertheless, this can involve high costs for the controllers and may hinder the entrance of smaller online service providers into the market. Maybe for this reason, the GDPR has not taken this requirement but has made a recommendation of it in its recital 68. It thereby encourages the data controllers to enable data portability by developing interoperable formats but without making it an obligation.¹⁹³

7.3.2. Without hindrance

The right to data portability under the GDPR enables the data subject to receive its personal data from the controller he provided it to and to transfer this data “without hindrance”. This implies for a strong form of data portability knowing the format in which the data has to be given by the data controller. This means that the data controllers will have the obligation to transfer the concerned data, which presupposes a prohibition for the data controllers to block technically the transfer of personal data by giving it in a format that cannot be reused. Because there is no standard

format defined by the GDPR, the data controller can choose the format it uses as long as it fulfils the requirements of article 20(1) of the GDPR.

7.3.3. Where technically feasible

According to article 20(2) of the GDPR, the right for the data subject to have his personal data transferred from one data controller to another is only given when it is technically feasible. This is a rather vague requirement as there is no additional explanation. Some believe that it might reduce the incentive for companies to enable data portability.¹⁹⁴ Indeed, companies could restrict data portability by making programs that make data portability technically not possible. Nevertheless, this is not the perspective of the GDPR when reading its recital 68. It encourages indeed data controllers to develop interoperable formats, which would enable and facilitate data portability. Therefore, companies have the responsibility to make their data portable and to choose the appropriate format. By leaving the choice to the companies, the Regulation is shifting the burden to come up with technical solutions to industries.¹⁹⁵ How the companies will deal with requirement is not clear yet.

7.4. Protection of personal data and privacy

The aim of the data portability right is to reinforce the control individuals have on their personal data.¹⁹⁶ Three matters of concern arise in this context.

First, concerns arise about who owns this data that has to be portable. This is particularly relevant in the field of social networks where people post pictures with friends or have friends lists. The intention of data portability would be to allow the transfer of those. The question here is how to deal with data that involves information about other individuals. A friends list could be a good example, as an individual may want to transfer its profile on a new social network site and therefore move its lists of friends. Consequently, the people in the friends list will be automatically transferred in the new social network. This has two consequences. First, this results in empty profiles, which is not useful for the new social network site. Secondly, this empty profile is out there, without the consent and knowledge of the concerned individual. The same issue arises for persons who wish to transfer their pictures to a new site. If several people are in this picture, would it be correct to let the individual transport this photo to a new site and therefore expose the other individuals? If it is, how can we control our data? These questions can already be asked, as the problem already exists in the context of social networking sites. Data portability would however increase this phenomenon.

A second related issue concerns the transfer of information that might be protected by intellectual property rights. An individual might be confronted with restrictions when willing

¹⁸⁵ General Data Protection Regulation, art 20, §1.

¹⁸⁶ Swire and Lagos (n 64) 345.

¹⁸⁷ *ibid.*

¹⁸⁸ *ibid.*

¹⁸⁹ <<http://www.europeandataportal.eu/en/content/goldbook/preparing-data>> accessed 08 May 2016

¹⁹⁰ Swire and Lagos (n 64) 346.

¹⁹¹ General Data Protection Regulation, recital 21.

¹⁹² De Graef, Verschakelen and Valcke (n 73) 55.

¹⁹³ General Data Protection Regulation, recital 68.

¹⁹⁴ Yuli Wahyuningtyas, ‘Data Portability Series: Homework to Be Done on the Way Forward’, (Media Policy Project Blog, 6 May 2014), <<http://blogs.lse.ac.uk/mediapolicyproject/2014/05/06/data-portability-series-homework-to-be-done-on-the-way-forward/>> accessed 10 September 2015.

¹⁹⁵ Wahyuningtyas (n 194).

¹⁹⁶ Council of the European Union (n 168) 2.

to transfer profile to another social network if this information contains videos, music or other similar data on which they do not have a copyright or license.

The third concern relates to the risk to privacy created by data portability. Some scholars are preoccupied by the action of some to transfer their data to a provider carrying less restrictive privacy requirements.¹⁹⁷ As some consider this a risk for the individuals, others believe this will strengthen the privacy protection, as sites with the better protection will be the more successful. Indeed, in this regard, Gabriela Zanfir, privacy and data protection law specialist states that even if there are additional safeguards for the subjects of processed data, “by ensuring data portability through established statutes, the individual enjoys a strengthened right to ‘informational self-determination’”.¹⁹⁸ In the same context, Ian Brown, Internet governance expert of the Oxford Internet Institute, believes that data portability will not harm privacy as the obligation of technical and organisational measures to protect data will still be applicable to the online service providers.¹⁹⁹

Both the European Commission and the European Parliament have failed to address these issues. Neither article 18 of the proposal for a GDPR, nor article 15(2) of the amended version of the proposal deal directly with privacy and intellectual property issues.²⁰⁰

Unlike the other European legislative Bodies, the Council did consider this subject. Article 15(2a) of the Council’s general approach on the proposal for a GDPR states that the right of the data subject to obtain a copy of its personal data undergoing processing by the controller shall not apply under two circumstances.

Firstly, if “such copy cannot be provided without disclosing personal data of other data subjects or confidential data of the controller”.²⁰¹ Secondly, “if disclosing personal data would infringe intellectual property rights in relation to processing of those personal data”.²⁰²

Unfortunately, this was not taken over in the GDPR. The right to data portability has one restriction in article 20(4) of the GDPR, which states that, it “shall not affect the rights and freedoms of others”. This is however a very broad statement which will have to be interpreted in the near future in order to avoid privacy and intellectual property issues.

8. Conclusion

Although the demand to make data portable is relatively clear, the best way to attribute this right is not. The right to data portability could be, as discussed in this article, granted through

two different ways. Firstly, through European Competition Law. Secondly, through the General Data Protection Regulation. The aim of this article was to analyse which approach could be more successful.

First, an analysis of European Competition Law was made where it was examined if it could be successfully applied to cases of data portability breaches creating an anti-competitive effect such as the lock-in of the data subject. It appears that this is a challenging task as the conditions for article 102 of the TFEU are burdensome and difficult to apply to online services. As a result, the chances for article 102 of the TFEU to apply to data portability cases seem restricted and therefore appear not to be the best way to attribute data portability in Europe.

Consequently, an analysis was made of U.S. antitrust law in order to determine whether it could be a source of inspiration for the European Legislative Bodies. Unfortunately, it has to be concluded that U.S. antitrust law does not go in favour of data portability. On the contrary, it seems to be harder to apply it to data portability, as case law is relatively restricted in this context.

Finally, the right to data portability was examined as it is stated in article 20 of the new General Data Protection Regulation. It is not clear to what extent article 20 will be applicable and enforceable as the General Data Protection Regulation has only been published recently and will enter into force in 2018. However, we do know that a first step towards portable data has been made. In my opinion, it is a move in the right direction to allow for a greater data portability right of the individual. When following the legislative procedure, it was rather unclear in which direction the final draft would go as the point of views of the European Legislative Bodies were differing in the context of data portability. However, the European Legislative Bodies have put a great effort in laying down principles and rules to grant a data portability right to the data subjects in the GDPR. It is indeed clear now that data subjects will have the right to obtain a copy of their personal data and to transfer it or have it transferred from one online service provider to another. Furthermore, the GDPR will have a broad scope of application, applying not only to companies with a dominant position, as it is required under European Competition Law, but to controllers or processors which provide means for processing personal data regardless if they are based in the EU or not.

While it is true that some key terms of the GDPR still need to be interpreted in order for it to grant the right to data portability effectively, I do believe it is the best chance for a right to data portability to be granted in Europe. As for the extent of this right as well as its actual application, only time will be able to tell.

Acknowledgement

The University of Vienna supported this article. I thank Professor Doctor Van Eecke for providing his insights and expertise during the research. Furthermore, I would like to thank Professor Saxby for his guidance when writing the article.

¹⁹⁷ Yoo (n 32) 1155.

¹⁹⁸ Zanfir (n 6) 152.

¹⁹⁹ De Graef and Wahyuningtyas, ‘Data Portability Series: Interview with Ian Brown’, (Media Policy Project Blog, 23 April 2014) <<http://blogs.lse.ac.uk/mediapolicyproject/2014/04/23/data-portability-series-interview-with-ian-brown/>> accessed 17 October 2015.

²⁰⁰ Swire and Lagos (n 64) 348.

²⁰¹ Council of the European Union (n 168) art 15 (2a).

²⁰² *ibid.*