HAL open science

Discussions on the Right to Data Portability from Legal Perspectives

Kaori Ishii

▶ To cite this version:

Kaori Ishii. Discussions on the Right to Data Portability from Legal Perspectives. 13th IFIP International Conference on Human Choice and Computers (HCC13), Sep 2018, Poznan, Poland. pp.338-355, 10.1007/978-3-319-99605-9_26 . hal-02001955

HAL Id: hal-02001955

https://inria.hal.science/hal-02001955v1

Submitted on 31 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Discussions on the Right to Data Portability from Legal Perspectives

Kaori Ishii[1]

[1] Faculty of Library, Information and Media Science, University of Tsukuba, Tsukuba, Japan
kaoriish@slis.tsukuba.ac.jp

Abstract. This study discusses the legal issues pertaining to data portability from the perspectives of both personal data protection and antitrust laws. Since legal challenges arise from the differences between antitrust law and data protection law, there is a need to define the legal position of data portability. My analysis is based on a review of these three topics: Is the right to data portability in the EU General Data Protection Regula-tion (GDPR) effective? (2) Should the right to data portability be legally regulated? and (3) Can the right be regulated from an antitrust perspective?

What are indicated from the above discussions are: (1) the right to data portability in the GDPR is the first promising provision which has given rise to several issues—in particular the scope of the data, IT costs imposed on SMEs, and theoretical boundaries and enforcements based between data protection and antitrust laws—that warrant fur-ther examination; (2) if the controller-controller portability is called for, antitrust per-spective broadly encompass the scope of data is preferred than data protection regula-tion; (3) combining data protection and antitrust perspectives into a single law would be difficult due to the differences of them; (4) when it comes to establish data portability scheme from antitrust perspective, data portability should be obliged depending on the kinds of platform.

Keywords: Data Portability, Privacy, Personal Data, Antitrust.

1 Introduction

This article discusses legal issues on the right to data portability both from personal data protection and antitrust perspectives, and provides some policy recommendations for formulating the right to data portability.

The EU General Data Protection Regulation (GDPR) [1] introduced a new right to data portability. One of its intentions is addressing data monopolization by "GAFA."[1] The European Commission (EU Commission) acknowledges the possible advantages of the right from a competition perspective because start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more con-

[1] GAFA is a buzzword meaning Google, Apple, Facebook, and Amazon.

sumers with privacy-friendly solutions, increasing competitiveness in the economy [2].

This right primarily empowers the control of personal data by a data subject, while simultaneously preventing vendor lock-in. The Article 29 Data Protection Working Party (WP29)[2] states that the data portability right facilitates data subjects' ability "to move, copy or transmit personal data easily from one IT environment to another," and also fosters competition between controllers in the context of the Digital Single Market strategy [3].[3]

Conversely, large and strong online platforms have already been established by giant U.S. internet companies, creating a need to question the framing of the right and identifying legal challenges.

The data portability right has been managed on a country basis. For instance, the French Digital Republic Act (une République numérique) enacted on October 7, 2016, introduced the right to data portability. The midata program launched in 2011 and backed by the UK government facilitates consumers' access to their personal data in a portable, electronic format. The Obama Administration launched a series of My Data initiatives in 2010. Comparing the right to data portability in the EU and efforts in other countries is helpful for devising policy recommendations and ensuring an objective discussion.

Legal challenges stem from the differences between the approach of antitrust law and data protection law. The former aims for fair and free competition by prohibiting private monopolization, unreasonable restraint of trade, and unfair trade practices. From this perspective, facilitating switching between IT providers may be preferable. The latter law aims at protecting personal data by granting the rights to data subjects. Data transactions are thus permitted only when the data subject's control is warranted. These differences lead to conflicts between enforcement agencies. Under certain conditions, a data protection authority may impose some restrictions against personal data transactions, but a regulatory agency in competition law may insist on personal data sharing among competitors. Thus, defining the legal positioning of data portability becomes important.

2 The Right to Data Portability

2.1 General Data Protection Regulation

The Right to Data Portability. Article 20(1) of the GDPR defines the right to data portability, granting the data subject the right to receive his/her personal data provided

---

[2] WP29 is composed of respective representatives of the supervisory authority (ies) designated by each EU country, the authority (ies) established for the EU institutions and bodies, and the EU Commission

[3] Digital Single Market is "one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence" [3].

to a controller, in a structured, commonly used, and machine-readable format, and the right to transmit those data to another controller without hindrance from the current controller [1]. Article 20(2) grants the data subject the right to have his/her personal data transmitted directly from one controller to another, where technically feasible. This right is close to the right of access already protected in the Data Protection Directive in 1995 [4], but it expands the right of access to direct transmission between controllers.

WP29 published Guidelines on the Right to Data Portability (last revised and adopted on April 05, 2017) [5]. It aims at clarifying the scope, conditions under which the right applies, and the scope of "personal data provided by the data subject." A directory of a data subject's contacts created by a webmail service, titles of books purchased online, or bank transactions to a service that manages budget are examples of data included in the scope of the right. WP29 notes that "the right to data portability is not limited to personal data that are useful and [is] relevant for similar services provided by competitors of the data controller[4].

Although WP 29 indicates that the term "provided by the data subject" must be interpreted broadly, "inferred data" and "derived data" such as the outcome of an assessment of user health or a profile created for risk management and financial regulations (e.g., to assign a credit score or comply with anti-money laundering rules) are excluded from this scope[5]. The term "provided by" includes personal data related to the data subject activity or results from the observation of an individual's behavior, but does not include data resulting from subsequent analysis of that behavior[6]. Personal data created by a personalization or recommendation process, by user categorization or profiling are derived or inferred data, resulting in the exclusion from the right[7].

WP29 interprets "hindrance," as it "can be characterized as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller"[8]. For instance, fees for delivering data and excessive delay fall under "hindrance"[9].

WP29 considers that "technical feasibility" should be assessed on a case-by-case basis. As Recital 68 of the GDPR does not oblige creating processing systems that are technically compatible, WP29 follows this by interpreting "portability aims to produce interoperable systems, not compatible systems"[10]. While WP29 does not identify the specific format, it strongly encourages cooperation between industry stakeholders and trade associations to devise a common set of interoperable standards and formats.

---

4 [5] p.6
5 [5] p.10
6 [5] p.10
7 [5] pp.10–11
8 [5] p.15
9 [5] p.15
10 [5] p.17

WP29 recognizes that the right will enhance competition between data controllers; but does not assure that the right will limit portable data to data necessary or useful for switching services[11].

2.2 Efforts in Member Countries

French Digital Republic Act. The French Digital Republic Act (une République numérique) enacted on October 7, introduces the definition of "digital platform" and the right of data portability [6].Article 48 of the Act (Article 224-42 of the Consumer Protection Code) requires any online public communication service provider to recover the following data for the con-sumer for free: all the files stored online by the consumer; all the data from using the consumer's user account and online account that is retrieved in an open standard, and is easily reusable and exploitable by an automated processing system; and other types of data associated with the user's online account that facilitate change of service pro-viders. The last type of data takes into account the economic importance of the services concerned, the intensity of the competition between the suppliers, the utility for the consumer, the frequency, and the financial stakes of the use of these services.

SelfData Initiatives. WP29 offers midata in the United Kingdom and MesInfos /SelfData by FING in France as examples of experimental applications in Europe.
The midata program was launched in 2011 with the support of the Department for Businesses, Innovation and Skills. According to the midata website, a midata file is a record of up to 12 months of transaction history of the customer's personal current accounts (PCA). On downloading their midata file, the customer can submit it to comparison providers, who analyze the data in the file and provide customized information. This may help identify possible account switching options [7]. The midata Innovation Lab (miL) was set up to promote the midata program in 2011; the areas of the project originally covered education, transport, and health [8]. Currently, the midata initiative focuses on banking data. GoCompare.com is the first comparison provider launched in March 2015 to offer customers current bank account switching, whose efforts are expected to promote the midata program [9].

MesInfos /SelfData project, launched in 2012, is a pilot project that collects, uses, and shares personal data by and for individuals, under their complete control and is designed to fulfil their needs and aspirations. In 2017, the project will take actions to make experiments into reality by providing a personal cloud with 3,000 testers; transmitting data on these testers to each personal cloud of several organizations including insurance, energy, and telecom providers; and adding more data by testers on their personal cloud to gain use value from their data [10].

[11] [5] p.4

2.3 Experiences in the United States

The United States. The Obama Administration launched a series of My Data initiatives in 2010 [11] that aim to provide all Americans easy and secure access to their own personal data, such as Blue Button for health data, Green button for electric utility data, and My Student Data for Federal student data. "Data portability" in this sense refers to enhancing "the ability to download the information that a service stores for or about an individual" [12]. However, unlike the GDPR, the term does not allow direct switching of providers.

The Obama administration asked for comments from stakeholders on issues including benefits and drawbacks, the need for governmental regulation, and health data in September 2016. The administration published comment summary in January 2017 and stated that "portability should be incentivized but not mandated." This means that additional government regulation is not necessary, since the market should not be regulated in a manner that is inefficient, ineffective, and not suitable to context-specific data portability needs, as they would move overseas to avoid overly burdensome regulations and new regulations would be premature for rapidly developing industries [13]. U.S. data portability is underlined by clear and transparent communication, thereby building individuals' trust.

3 Antitrust Laws and "Essential Facilities" Doctrine

3.1 The United States

Sherman Act. The right to data portability can be analyzed from the antitrust law perspective, as undertakings that refuse to move data to another undertaking may constitute a "refusal of deal." The U.S. first discussed this issue. Before the enactment of the Sherman Act in 1890, some court decisions had imposed "duty to deal" on public busi-nesses such as a railway company or a shipping company [14].

Article 1 of the Sherman Act punishes any contract in restraint of trade or commerce; and Article 2 punishes monopolization, attempt to monopolize, and conspiracy to monopolize (15 U.S.C. §§ 1, 2). Refusal of a deal by a large online platform or platforms may contradict these provisions; however, this is deemed unlawful in exceptional circumstances. The U.S. Supreme Court, in the United States v. Colgate & Co. (1919), held that "in the absence of any purpose to create or maintain a monopoly, the act does not restrict the long recognized right of trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal" [15]. This ruling was followed by the Trinko decision in 2004. Contrary to the Aspen decision in 1985 that indicated a refusal to cooperate with rivals as a violation of Article 2 [16], the Supreme Court in Trinko held that "we have been very cautious in recognizing such exceptions, because of the uncertain virtue of forced sharing and the difficulty of identifying and remedying anticompetitive conduct by a single firm", "the few existing exceptions from the

proposition that there is no duty to aid competitors"[12]. Opposing this ruling, the Department of Justice and the Federal Trade Commission (FTC) jointly argued that "if such a refusal involves a sacrifice of profits or business advantage that makes economic sense only because it eliminates or lessens competition, it is exclusionary and potentially unlawful," citing the Aspen decision [18]. Thus, "refusal of deal" remains controversial. If following the ruling in Trinko, a refusal of data portability by a single dominant may not be deemed unlawful.

Refusal of data access has been disputed in some cases[13]. In LiveUniverse v. MySpace (2007), LiveUniverse alleged that MySpace prevented users from watching vidiLife videos that they or other users previously had loaded onto their MySpace webpage, violating Article 2. The District Court dismissed the claims as a company generally has a right to deal, or refuse to deal, with whomever it likes, as defined in the Trinko decision [20]. The District Court's dismissal was affirmed by the U.S. Court of Appeals. In Facebook v. Power Ventures Inc., Facebook alleged that Power accessed the Facebook website to extract all kinds of social networking contacts of users from its platform in violation of its terms of use, and when Facebook attempted to stop Power's unauthorized access, Power circumvented Facebook's technical barriers. The district court dismissed Power's claim that Facebook maintained monopoly power by threatening potential new entrants to the social networking market [21]. In PeopleBrowsr v. Twitter, PeopleBrowsr asked Twitter to grant it (full firehose) access to Twitter data to be able to offer analytics services and was denied this request. The parties resolved the case, and PeopleBrowsr was given firehose access through the end of 2013 [22] [23]. Vanberg and Ünver comment that US antitrust law and principles took a divergent path from mandatory access obligations, particularly after Trinko decision [19]. They argue that "proving the 'indispensability' or 'essentiality' of the requested input often poses the main difficulty for the plaintiffs to overcome" [19, para. 3.3.2].

Essential Facilities Doctrine. Information monopolization raises concerns about the "Essential Facilities" doctrine, which was developed in the 1970s. The theoretical back-ground supporting the doctrine include the bottleneck theory facilitated by A.D. Neale [24], and the "public utility" facilitated by L.A. Sullivan [25].[14]

This principle derives from the Terminal R. Association ruling in 1912 [26], in which nonmembers of the defendant's joint company were refused access to railway terminal facilities. The ruling held that the building unified system of terminals violated Articles 1 and 2 of the Sherman Act, said to be the first leading case applied by the essential facilities doctrine. The doctrine was reaffirmed in other decisions [27].

---

[12] [17] pp.408, 411

[13] [19] para. 3.3.2

[14] "[I]f a group of competitors, acting in concert, operate a common facility and if due to natural advantage, custom, or restrictions of scale, it is not feasible for excluded competitors to duplicate the facility, the competitors who operate the facility must give access to the excluded competitors on reasonable, non-discriminatory terms," L. A. Sullivan [25] § 48, at 131.

While this doctrine typically encompasses physical facilities, the Sherman Act applies to the refusal of access to electronic network systems [28].

The first court case explicitly acknowledged the "essential facilities" doctrine was the Hetcht case [29]. The District of Columbia Circuit defined the doctrine by citing Neale's article, stating that "where facilities cannot practicably be duplicated by would-be competitors, those in possession of them must allow them to be shared on fair terms. It is illegal restraint of trade to foreclose the scarce facility"[15]. However, the Trinko decision refused to apply the doctrine stating that it had never recognized nor intended to recognize it[16].

3.2 The European Commission

Treaty on the Functioning of the European Union. The EU has a history of antitrust law that is less intensive than the U.S. Article 101 of the Treaty on the Functioning of the European Union (TFEU) [30] prohibits agreements, decisions, and concerned practices that may affect trade between Member States and prevent competitions. Article 102 prohibits abuse by one or more undertakings in a dominant position. Articles 101 and 102 succeeded Articles 81 (ex-81) and 82 (ex-86) of EC Treaty (Treaty of Rome) in 1957 with the conclusion of the Lisbon Treaty in 2009.

The dominant position was clarified in the Hoffmann case in 1979 [31]. The European Court of Justice (ECJ) defined abuse is an objective concept relating to the behavior of an undertaking in a dominant position that influences market structure in a manner that weakens the degree of competition and hinders the maintenance of the degree of competition still existing in the market or the growth of that competition [31, para 91]. The judgment in the European Court (fifth chamber) in another case interpreted an abuse as occurring when without any objective necessity, an undertaking holding a dominant position on a particular market reserves to itself an ancillary activity that could have been carried out by another undertaking as part of its activities on a neighboring but separate market, which could potentially eliminate all competition from such undertaking[17]. The refusal to enable data portability by a dominant firm is seen as "a form of exclusionary abuse as it might drive its competitors out of a specific relevant market and increase market concentration"[18].

Essential Facilities Doctrine in the EU. The EU has adopted the essential facilities doctrine from the U.S. Sherman Act. If a monopolist refuses "to provide other firms with access to something that is vitally important to competitive viability in a particular market," it constitutes a violation of Article 1 and 2 of the Sherman Act.[19] Renowned scholar Dr. Temple Lang notes a fundamental view to establish responsibility for refusal of access under the doctrine. He states the following: (1) competi-

---

[15] [24] p. 67
[16] [17] pp.410–411
[17] [32] para 27
[18] [19] para 3.2
[19] [33] p.87

tion law does not require companies to give their competitors access to their assets, net-works, or intellectual property; (2) this is same under both Articles 101 and 102 of the EC Treaty, under the "essential facilities" principle; (3) "this principle applies only if the refusal to give access has serious anticompetitive effects, if access is essential to enable competitors to compete, and if there is no legitimate business justification for the refusal"[20]. He further elaborates by stating, "The principle applies only where the facility cannot be duplicated at all by competitors, even if acting to-gether, for legal, economic or geographical or other physical reasons, and where the refusal to contract would eliminate competition in a downstream market for which ac-cess to the facility is necessary, and not merely advantageous"[21]. As the U.S. Supreme Court cautiously limits the scope of the doctrine, interpretations in the EU also appear restrictive.

In Commercial Solvents, the ECJ first found the denial of deal owing to abuse of dominant position according to Article 86 (currently 102). Commercial Solvents was a monopolist manufacturer of chemical raw materials who refused to supply material to a regular customer and competitor on the downstream market, thereby risking all competition on the part of this customer. Other court cases have also developed this doctrine through denial of access [36].

The European Commission expressly declared the criteria for an "essential facility" in B&I Line v. Sealink case (1992). The European Commission held that "a dominant undertaking which both owns or controls and itself uses an essential facility, i.e., a facility or infrastructure without access to which competitors cannot provide services to their customers, and which refuses its competitors access to that facility or grants access to competitors only on terms less favorable than those which it gives its own services, thereby placing the competitors at a competitive disadvantage, infringes Article 86, if the other conditions of that article are met"[22].

In the Magill case, three Irish broadcasting companies refused to share weekly listings of TV programs to the Magill TV Guide. The ECJ in 1995 held that this refusal prevented constitutes an abuse under Article 86 (current 102)[23]. Similar to U.S. courts, this decision implicates that intangible obstacles can impediment new entries to the market.

In IMS Health (2015), the ECJ presented restrictive conditions to ensure that a refusal to deal is treated as abuse: (1) the refusal relates to a product or service that is indispensable for carrying on a particular business; (2) the refusal prevents the emergence of a new product with a potential consumer demand; (3) it is unjustified and aims to exclude any competition in a secondary market[24,25]. Inge Graef et al. noted that similar to the U.S. antitrust law, dominant undertakings can decide freely with whom they wish to deal under the abuse of the dominance regime of European com-

---

[20] [34] S117-118
[21] [35] p.21
[22] [37] para 41
[23] [38] para 53–54
[24] [39] para 38
[25] This ruling is confirmed in Microsoft case [41], para. 332.

petition law. Only in exceptional circumstances can an obligation to contract be imposed based on the essential facilities doctrine[26].

The ECJ held in Microsoft (2007) that "non-Microsoft work group server operating systems must be capable of interoperating with the Windows domain architecture on an equal footing with Windows work group server operating systems if they were to be marketed viably on the market"[27]. This was a specific case of Microsoft almost holding a dominant position in the relevant market, and a considerable legal burden had to be met particularly with regard to proving the indispensability of the data to which access is sought[28]. Regarding this, Lang strongly distinguishes the position of Microsoft and Google on the account of the nature of the product or service, the essentiality of the product or service, the burden of switching cost, and the existence of network effects. He defines a "platform" as "a combination of hardware and software on the basis of which other companies (software vendors in the Microsoft case, and advertisers in the Google case) offer products and services to end customers in competition with one another." He identified Windows as Microsoft's platform and the Internet as that of Google. The contrasts between Microsoft's Windows and Google's Internet are: Microsoft charges users and Google offers free services; software developers must be available on Windows, while publishers can reach consumers through a variety of services other than Google; switching cost is high in the case of Microsoft and it is negligible in the case of Google; there were important network effects in Microsoft case, while there do not seem to be any network effects for search activities[29,30]. His argument clearly denies Google's dominant position and thereby rejects that it is an essential facility.

3.3 Merger Cases Bridging Privacy and Anti Competition

Some merger cases take into account privacy affects. In re Google-DoubleClick (2007), both the European Commission [42] and the FTC [43] referred to the effects on privacy. While the European Commission separated the merger decision and legal obligations in the 1995 Data Protection Directive [4] etc., it permitted internet service providers to track all the online behavior of their users and stated that large internet service providers could team up with advertisement companies to utilize such data within the confines of privacy rules, but that with customers' consent, they could use such data, for instance, in exchange for lower prices[31]. Though the FTC also approved the merger, two members expressed privacy concerns raised owing to the production of highly sophisticated targeting data by combining both companies [44] [45]. In re Microsoft-LinkedIn (2016), the European Commission acknowledged that data priva-

---

[26] [40] p.382

[27] [41] para 421

[28] [41] pp.382–383

[29] [35] pp.7–9

[30] Google case seems to be related to the case that the European Commission fined Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service, on June 27th, 2017.

[31] [42] para 271

cy was an important parameter of competition in the SNS service market. It stated that privacy-related concerns could be considered in competition assessment "to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor" [46]. A privacy concern would arise if both undertakings' user databases are integrated, as this could shut out LinkedIn's competitors from accessing Microsoft's API, which they need to access user data stored in the Microsoft cloud [46].

Facebook's misleading practice caused the European Commission in 2017 to fine it €110 million for providing incorrect or misleading information during the Commission's investigation under the EU Merger Regulation [47]. Facebook made a commitment in 2014 that it would not establish reliable automated matching between Facebook and WhatsApp users' accounts [48]. However, in 2016, WhatsApp announced updates to its terms of service and privacy policy, contradicting the said Facebook commitment.

The European Commission fined Google €2.42 billion for breaching EU antitrust rules in 2017. Google was found to have abused its market dominance as a search engine by promoting its own comparison shopping service in its search results, and demoting those of competitors, thereby depriving consumers of genuine choice of services. The Commission held that search engine markets in all EEA countries had been monopolized by Google, which had high market shares exceeding 90 percent in most countries since 2011. The more consumers use a search engine, the more attractive it becomes to advertisers, resulting in attracting even more consumers and improving results. This creates high barriers for entering the market [49]. The European Commission also noted two preliminary findings in 2016 with respect to the Android operating system and AdSense that Google had abused its dominant position [50, 51].

4 Discussion

4.1 Issues for Discussion

The above discussion identifies the following issues: (1) Is the right to data portability in the GDPR effective? (2) Should the right to data portability be legally regulated?; (3) Can the right be regulated from an antitrust perspective?

4.2 Is the Right to Data Portability in the GDPR Effective?

While the right to data portability is already provided in the GDPR, the right has not strongly influenced countries' legislations other than the EU member states. This right is critically reviewed by Vanberg and Ünver[32]. They list six issues: (a) limitations on data generated by the data controller; (b) privacy rights of third parties; (c) technical feasibility of data transfer; (d) disproportionate costs and efforts; (e) transfer of data may compromise valuable proprietary information and intellectual privacy; (f) en-

[32] [19] para. 2.1

forcement issues pertaining to the right to data portability; and (g) privacy and data security risks.

Authors argue regarding Issue (a) that an auction website such as eBay allows users to only move their personal data and not their ratings and reputation to another auction site, as the latter is provided by the service provider[33]. Issue (b) is illustrated in a photograph on Facebook in which several people appear; one data subject cannot import it to another social networking platform, as others appear in the picture[34]. Collaboration among market players is suggested to address Issue (c). Regarding Issue (d), many small- and medium-sized companies (SMEs) do not have the resources to be aware of the GDPR overall compliance, and write a corresponding software to move data to another provider. Not only is data portability costly, but also IT costs on SMEs will be significantly increased by the EU data protection reform[35]. Issue (g) pertains to the burden imposed on SMEs. In Issue (e), authors illustrate a case impeding a business model of an online digital service that helps users of online clothing retailers. If such a service provider is required to move data including detailed personal data specific to its services, this will clearly have a stifling effect on competition and innovative solutions. To address Issue (f), authors question legal and theoretical boundaries between the right and other laws, as well as enforcements. According to their analyses, the GDPR data portability is ineffective.

Swire and Lagos made a critical approach to the right to data portability [52]. They analyzed this right in the GDPR draft stage under antitrust or competition law, data protection, and privacy perspective, and pointed out several flaws as below.

The right to data portability is far broader than competition law as the right is considerably over broad and reduces consumer welfare. Despite the difficulty of demonstrating exclusionary practices including refusal to apply, denial of access to an essential facility, or a tying violation under European law, the right to data portability ignores arguments about substantial efficiency. The differences between the right to data port-ability and competition law are elaborated as follows: "[f]irst, the RDP [the right to data portability] does not require a showing of market power and applies equally to monop-olies and to small and medium enterprises. Second, the RDP uses a per se approach that does not compare the precompetitive efficiencies against the harms to competition. Third, failure to write EIM [export–import module] software does not fit under the tra-ditional categories of exclusionary conduct prohibited by current competition law"[36]. Ensuring interoperability is considerably hard to achieve even with Open Document Formats. The right to portability would impose substantial costs on suppliers of software and apps, which would then be passed on to consumers[37]. Competition law does not require the first service provider to write the EIM, as the exclusionary practices trigger sanctions only when there is a particularized show-

[33] The authors referred to Inge Graef et al. [40].
[34] This case is illustrated by Barbara Engels [55] as below referenced.
[35] This issue has been intensively discussed in Swire and Lagos [52].
[36] [52] pp. 350–351
[37] [52] pp. 354–356

ing in a specific market of harm to consumers, and the legal rule establishes high thresholds for the application of the essential facilities doctrine[38].

The authors also raised legal challenges to the right to data portability from the perspectives of data protection and privacy. They argued that the right is not well established, no jurisdiction has experimented with anything resembling the right, and the right appears to essentially be normal legislation and regulation rather than part of the constitutional process despite the human right or the fundamental right argument in the EU[39]. In particular, the serious risk that the right would pose to security must be noted among their arguments. They assert that "one-time access to a site, such as by a hacker, can turn into a lifetime's download of data from that site. Defining the RDP, therefore, should be done with full awareness of risks to the right to data security"[40].

WP29 has partially responded to the above concerns. The guidelines allow controllers to transmit the entire directory of incoming and outgoing e-mails when switching a webmail service, or to move both the account holder and the remitters' information when transmitting bank account information. Collaboration among market players to overcome technical feasibility of data transfer is agreed by WP29 guidelines. WP29 indicates some authentication such as a shared secret, a onetime password, or suspend-ing or freezing the transmission in addition to general risk mitigation measures. How-ever, these measures are already implied in Article 5(1)(f) of the GDPR. It does not condition specific security measures on transmitting data[41].

Contrary to the narrow interpretation of the scope of the data, the European Commission expressed its concern over the overly broad interpretation of EU privacy regulators, because including observed data and raw data extend beyond what has been agreed upon in the legislative process. Observed data was one of the most controversial aspects of the guidelines.

4.3 Should the Right to Data Portability be Legally Regulated?

Legally regulating the right to data portability gives rise to three options. The first is to limit personal data by stipulating the right in an act to protect personal data, the second is to encompass a broad range of data by stipulating the right in an act to anti-competition. The third is to enact a new law incorporating both perspectives.

The GDPR preceded an anti-competition act. Although the right to data portability in the GDPR has led to controversial issues, this new incorporation is very promising, as it significantly empowered the data subject. Other countries have encouraged voluntary efforts. The United States resorts to voluntary efforts, as it considers that portability should be incentivized but not mandated. The U.K. and France have also engaged in self-data approaches, some of which are backed by governmental agencies. It should be noted that they aim to help consumers access and use data collected about them by service providers, and not to directly switch data between undertakings.

---

[38] [52] pp. 360–365
[39] [52] pp.365–373
[40] [52] p.373
[41] [5] pp. 11, 18–19

Vanberg and Ünver emphasize the importance of controller–controller data transfer and request clear guidelines from the WP29, such as "what is meant by technically feasible, what is meant by data provided by the data subject himself/herself, as well as clarifying the delimitations of the right to data portability" [19, para. 5]. My argument is that controller–controller portability cannot be obliged from data protection perspective, as such obligation excessively impedes the economic rights of data controllers and imposes unnecessary legal burden on them. GDPR included "technically feasible" in controller–controller portability to address the above concerns. Moreover, the purpose of data protection is to protect individual's right, and not to foster competitive environment. If data portability is based on data protection, the structure of the right has to be established under the control of an individual, in addition to the scope of data being limited to personal data.

This article does not necessarily encourage legislative proposal on data portability, but it considers legal obligations from antitrust perspective might be needed if controller–controller portability should be achieved. Concerning the third pattern of regulation, the Digital Republic Act in France is a leading example. This act can include non-personal data portability, as it takes into account the economic importance of the services concerned, and the right includes "all the files stored online by the consumer." The European Commission encourages introducing a general right to data portability for non-personal data, considering that the right "could be seen as a possible means to enhance competition, stimulate data sharing and avoid vendor lock-in".[42]

As some merger cases pertain to privacy concerns, there are possibilities of bridging privacy and anti-competition, even as discrepancies exist between them. For instance, if a dominant online platformer seeking to combine customer data with another company contradicts its previous statements, it may be fined. Regarding personal data, enforcement policies by a competitive regulator and a data protection authority must be considered. In principle, rejection of access to personal data is not usually deemed illegal as the basic concept of an act on protecting personal data restricts disclosure of personal data from a business entity to a third party. A dominant company will be liable to the violation of access refusal against an antitrust law only when there is no issue from the personal data protection perspective, since individuals have provided their consent to the disclosure. In other words, when a company holds a dominant power in a certain market, data collected through business activities in the market play an indispensable role in businesses, and obtaining alternative data is technically and economically difficult, then unreasonable rejection to data access request by others may violate an antitrust law[43].

However, Swire et al. point out "important aspects of ICT industries suggest that a rule that mandates interoperability will often reduce innovation"[44]. As MySpace replaced Friendster and later Facebook took the MySpace dominant position, successive dynamic competition in the technology space comes from Joseph Shumpeter's "crea-

---

[42] [53] pp.46–49

[43] This issue was discussed in the expert committee in the Fair Trade Commission of Japan [54].

[44] [52] p. 358

tive destruction”[45]. As a result, obligatory data portability based on the anti-competitive perspective is not a simple solution.

4.4 Can the right be regulated from an antitrust perspective?

Considering antitrust laws and discussions of the essential facilities doctrine, a “duty to deal” cannot be easily granted to a competitor, as the principle of freedom of trade poses high legal barriers.

Barbara Engels analyzed the right to data portability from a competition policy [55]. She argued that “it is recommendable or at least not harmful to competition to make data portability obligatory when platforms offer complementary services. Furthermore, data portability can be recommendable when market players offer substitute products and one player is dominant due to anticompetitive conduct”[46]. For platforms offering essentially the same products (substitutes), data portability is desirable if market dominance is abused, as portability reduces the risk of customer lock-in. By contrast, data portability is harmful if there is no abusive anticompetitive conduct, since SMEs would be precluded from gaining returns on investments. Enforcements through competition law are preferable[47]. For platforms offering complementary services (e.g., a trading and a payment platform), data portability obligatory is recommendable or not harmful when platforms offer complementary services. Further, when market players offer substitute products and one player is dominant due to anti-competitive conduct, data portability can be recommendable. Conversely, where there is no anticompetitive conduct resulting in market dominance, data portability should not be obligatory but rather enforced through competition law if necessary. However, these conclusions need to be interpreted in a nuanced fashion on the timeframe and on the type of innovation[48].

Engels researched anti-competitive behaviors in online markets by mapping the category of platform markets and economical aspects including network effects economics of scale, differentiation, congestion, switching costs, and market concentration. In search engine markets, positive direct network effects are low, positive indirect network effects are high, and economics of scale are also high, the degree of differentiation is low, congestion is low, and switching costs are medium. What should be noted is that the market concentration is high, which increases the risk of dominance abuse. Therefore, search engines should focus on a data portability regulation. In the case of trading platforms and social network markets, data portability should be obligatory only when they are particularly large and offer complementary or substitute products. The author remarks that contrary to the ex-ante regulation of the right to data portability, ex-post enforcements based on competition law are also possible.

---

[45] [52] p. 358
[46] [55] pp. 9,13
[47] [55] pp. 7,10,13
[48] [55] pp. 9–10

According to her, the right to data portability should be interpreted in a tailored manner as well as be dependent on the type of platform[49].

5 Conclusion

Data portability is a right crossing data protection and competitive perspectives. As the right to data portability in the GDPR is explained based on the fundamental human rights, WP 29 does not clearly state the effects of the right on fostering competition. As Engels pointed out, "Data portability could significantly strengthen innovation by making data more available - but it could also hamper innovation by making data too available. A clear correlation is not detectable and thus should also not be suggested by the GDPR"[50].

According to the above analyses by Vanberg and Ünver, and Swire and Lagos, the current GDPR provision seems to be ineffective. If the right to data portability intends to adjust to anti-competitive perspective, the obligations must not be equally applied to large platformers and SMEs, rigid authentication methods have to be explored, and intensive examinations on the inter-operative format should be elaborated.

Engels proposes that data portability should be interpreted in a tailored manner as well as dependent on the type of platform. Though there is not an established definition on how "platformers" can be defined, Lang's definition is informative as a general term.

This article does not necessarily criticize the obligatory right to data portability, but proactive efforts to overcome the above issues are imperative. In particular, the possibility of controller–controller portability should be pursued. In terms of personal data protection, data portability must be analyzed on the basis of each individual; thereby the scope of the discussion is inevitably narrowed. By contrast, competitive perspective does not limit the range of data, and it can encompass the obligatory controller–controller portability. When it comes to examining such a right to portability, ensuring that data would not be gathered by large enterprises and clarifying legal conditions on imposing sanctions should be considered essential.

In sum, what are indicated from the above discussions are: (1) the right to data portability in the GDPR is the first promising provision which has arisen a lot of discussions issues, in particular the scope of the data, IT costs imposed on SMEs, and theoretical boundaries and enforcements based between data protection and antitrust laws, need to be further examined; (2) if the controller–controller portability is called for, antitrust perspective broadly encompass the scope of data is preferred than data protection regulation; (3) combining data protection and antitrust perspectives into a single law would be difficult due to the differences of them; (4) when it comes to establish data portability scheme from antitrust perspective, data portability should be obliged depending on the kinds of platform.

To achieve effective data portability, controller–controller transfer is preferable, and by following certain conditions, an antitrust regulatory scheme can be imple-

[49] [55] pp. 13–14
[50] [55] p. 13

mented. While this right does not overcome the monopoly owned by digital giants, it is expected to foster sound data flow using existing data platforms.

Acknowledgements. I would like to thank Ms. Mika Nakashima for assisting me with this study by providing useful information. This work was supported by JSPS KAKENHI Grant Number 15K03237.

References

1. European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L 119, pp. 1–88
2. European Commission. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
3. European Commission. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
4. European Union (1995) 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 pro-cessing of personal data and on the free movement of such data. Official Journal L 281, pp. 31–50
5. Article 29 Data Protection Working Party (2017) Guidelines on the right to data portability. Retrieved from http://ec.europa.eu/newsroom/just/item-de-tail.cfm?item_id=50083
6. The Law Number 2016-1321, The Digital Republic Act of October 7, 2016 (1) https://www.legifrance.gouv.fr/af-fichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id
7. PCA midata. http://www.pcamidata.co.uk/
8. Department for Business Innovation & Skills. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262271/bis-13-1314-the_midata-inno-vation-opportunity-v2.pdf
9. GoCompare. http://www.gocompare.com/money/midata/
10. MESINFOS. http://mesinfos.fing.org/
11. White House (2016) My Data: Empowering All Americans with Personal Data Access. https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empower-ing-all-americans-personal-data-access
12. White House (2016) Exploring Data Portability. https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability
13. White House (2017) Summary of Comments Received Regarding Data Portability. https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-re-ceived-regarding-data-portability
14. State v. Hartford & New Haven R.R. Co., 29 Conn. 538 (1861), Texas Express Co. v. Texas & Pacific Ry. Co., 6 F. 426 (C.C.N.D. Tex. 1881), Southern Express Co. v. Memphis, etc. R. Co., 8 F. 799 (C.C.E.D. Ark. 1881)
15. United States v. Colgate & Co., 250 U.S. 300, 307 (1919).
16. Aspen Skiing Co. v. Aspen Highlands Skiing Corp. 472 U.S. 585 (1985).
17. Verizon Communications, Inc. v. Law Office of Curtis v. Trinko, LLP, 540 U.S. 398 (2004).

18. The Statement Made by the Department of Justice and Federal Trade Commission in Trinko Case. http://supreme.findlaw.com/supreme_court/briefs/02-682/02-682-mer-ami-usa.html
19. Vanberg, AD& Ünver, MB, (2017) The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?. European Journal of Law and Technology 8(1).
20. LiveUniverse, Inc. v. MySpace, Inc., (C.D. Cal. June 4, 2007), affirmed by 304 Fed. Appx. 554 (9th Cir. December 22, 2008)
21. Facebook, Inc., Plaintiff, v. Power Ventures, Inc., et al., 2010 U.S. Dist. LEXIS 93517 (N.D. Cal. July 20, 2010).
22. PeopleBrowsr. http://blog.peoplebrowsr.com/2012/11/peoplebrowsr-wins-tempo-rary-restraining-order-compelling-twitter-to-provide-firehose-access/
23. PeopleBrowsr (2013) PeopleBrowsr and Twitter settle Firehose dispute http://blog.peoplebrowsr.com/2013/04/peoplebrowsr-and-twitter-settle-firehose-dispute/
24. Neale AD (2d ed., 1970) The Antitrust Laws of the United States of America.
25. Sullivan LA (1977) Handbook of the Law of Antitrust (Hornbook series).
26. United States v. Terminal Railroad Association, 224 U.S. 383 (1912).
27. Associated Press v. the United States, 326 U.S.1 (1945).
28. Otter Tail Power Co. v. United States, 410 U.S. 366 (1973).
29. Hetcht v. Pro-Football Inc., 570 F.2d 982 (1977).
30. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2007) Official Journal C 326: 1–390
31. Case 85/76 Hoffmann-La Roche & Co. AG v Commission of the European Com-munities (1979) ECR 461.
32. Case 311/84 CBEM v. CLT and IPB (1985) ECR 3261.
33. OECD (1996) The Essential Facilities Concept. http://www.oecd.org/competition/abuse/1920021.pdf
34. Lang JT (1999) Competition Law and Regulation Law from an EC perspective, Fordham International Law Journal 23(6): S116-S121
35. Lang JT (2016) Comparing Microsoft and Google: The Concept of Exclusionary Abuse, World Competition 39(1) pp. 5–28.
36. Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission of the European Communities (1974) ECR 223.
37. Commission Decision of 11 June 1992 relating to a proceeding under Article 86 of the EEC Treaty (IV/34.174-Sealink/B&I-Holyhead: Interim measures). http://ec.europa.eu/competition/antitrust/cases/dec_docs/34174/34174_2_2.pdf
38. Joined Cases C-241/91 and C-242/91 Radio Telefis Eireann (RTE) and Independ-ent Television Publications Ltd (ITP) v. Commission of the European Communities (1995) ECR I-743.
39. Case C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, (2004) ECLI:EU:C:2004:257.
40. Graef I, Wahyuningtyas SY, Valcke P (2015) Assessing data access issues in online platforms, 39 Telecommunications Policy, pp. 375–387. http://dx.doi.org/10.1016/j.telpol.2014.12.001
41. Case T-201/04 Microsoft Corp. v Commission of the European Communities (2007). http://curia.europa.eu/juris/liste.jsf?num=T-201/04
42. Case COMP/M.4731 Merger Case on Google and DoubleClick (2007). http://ec.europa.eu/competition/mergers/cases/deci-sions/m4731_20080311_20682_en.pdf
43. Statement of Federal Trade Commission Concerning Google/DoubleClick (2007).

https://www.ftc.gov/system/files/documents/public_state-ments/418081/071220googledc-commstmt.pdf
44. In the matter of Google/DoubleClick Dissenting Statement of Commissioner Pam-ela Jones Harbour (2007). https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf
45. Concurring Statement of Commissioner Jon Leibowitz Google/DoubleClick (2007). https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-state-ment-commissioner-jon-leibowitz-google/doubleclick-matter/071220leib_0.pdf
46. European Commission (2016) Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions. http://europa.eu/rapid/press-re-lease_IP-16-4284_en.htm
47. European Commission (2017) Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. http://eu-ropa.eu/rapid/press-release_IP-17-1369_en.htm
48. European Commission (2014) Mergers: Commission approves acquisition of WhatsApp by Facebook. http://europa.eu/rapid/press-release_IP-14-1088_en.htm
49. European Commission (2017) Antitrust: Commission fines Google €2.42 billion for abus-ing dominance as search engine by giving illegal advantage to own compar-ison shopping service. http://europa.eu/rapid/press-release_IP-17-1784_en.htm
50. European Commission (2016) Antitrust: Commission sends Statement of Objec-tions to Google on Android operating system and applications. http://eu-ropa.eu/rapid/press-release_IP-16-1492_en.htm
51. Antitrust: Commission takes further steps in investigations alleging Google's com-parison shopping and advertising-related practices breach EU rules http://eu-ropa.eu/rapid/press-release_IP-16-2532_en.htm
52. Swire P, Lagos Y (2013) Why the right to data portability likely reduces consumer wel-fare: Antitrust and privacy critique. Maryland Law Review, 72(2): 335–380
53. European Commission (2017) Staff Working Document on the free flow of data and emerging issues on the European data economy. https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy
54. Fair Trade Commission (2017) Expert Committee Report on Data and Competition Policy. http://www.jftc.go.jp/cprc/conference/index.files/170606data01.pdf (in Japanese)
55. Engels B (2016) Internet Policy Review 4. http://policyreview.info/articles/analy-sis/data-portability-among-online-platforms