Comparison of Legal Systems for Data Portability in the EU, the US and Japan and the Direction of Legislation in Japan

Mika Nakashima

▶ **To cite this version:**

Mika Nakashima. Comparison of Legal Systems for Data Portability in the EU, the US and Japan and the Direction of Legislation in Japan. 15th IFIP International Conference on Human Choice and Computers (HCC), Sep 2022, Tokyo, Japan. pp.159-169, 10.1007/978-3-031-15688-5_14 . hal-04395464

HAL Id: hal-04395464
https://inria.hal.science/hal-04395464v1

Submitted on 15 Jan 2024

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

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Comparison of Legal Systems for Data Portability in the EU, the US and Japan and the Direction of Legislation in Japan

Mika Nakashima [0000-0002-4265-5414]

Faculty of Global Informatics, Chuo University, Tokyo, Japan
nakashima.77h@g.chuo-u.ac.jp

Abstract. The General Data Protection Regulation (GDPR) is legislation for the protection of personal data that applies in the EU. Article 20 of the GDPR stipulates the Right to data portability as one of the rights of data subjects. The monopoly on data held by digital platforms, such as GAFA (Google, Amazon, Facebook, Apple), is becoming a significant issue, and in this context, there is a need for the right to data portability in terms of not only the right of data subjects to reclaim their personal data but also promoting competition among businesses. The California Consumer Privacy Act (CCPA) of 2018 is the first comprehensive legislation for the protection of personal data in the US, albeit at the state level, with provisions similar to the EU GDPR; the CCPA establishes the Right of access and portability in Section 1798.100 as one of the rights of consumers. The California Privacy Rights Act (CPRA), passed in 2021, amends the CCPA to further strengthen the rights stipulated therein. The Bill of the Consumer Online Privacy Rights Act of 2019 (CORPA) was introduced in the Congress in 2019 and may become the first comprehensive legislation for the protection of personal information in the US at the state level. In recent years, in addition to the GDPR in the EU and the CCPA, the CPRA and the CORPA in the US, provisions relating to the obligation of data portability from the perspective of policy on competition are also included in the new Digital Markets Act (DMA) proposed in the EU and the (federal-level) ACCESS proposed in the US. This study compares the legal systems of the EU, the US and Japan with regard to data portability and shows the direction of legislation in Japan.

Keywords: Data Portability, GDPR, CCPA, CPRA, CORPA, DMA, ACCESS

1 Legal Systems for Data Portability in the EU, theUS and Japan

1.1 The EU

The General Data Protection Regulation (GDPR)[1] was adopted on 27 April 2016, as a new legislation for protection of personal data replacing the Data Protection Directive (Directive); the GDPR came into effect on 25 May 2018, and it stipulates the Right to data portability in Article 20 as one of the rights of data subjects.

> Article 20 Right to data portability
>
> 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
> (a) the processing is based on consent pursuant to point (a) of Article 6 (1) or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and
> (b) the processing is carried out by automated means.
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
> 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
> 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

The guidelines developed by the Article 29 Working Group (2017), which was established under the Directive, outline the nature of the right to data portability as follows: [1, pp.4-5] [2]

> Firstly, data portability is a right of the data subject to receive a subset of the personal data processed by a data controller concerning him or her and to store those data for further personal use.
> …

[1] 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 the free movement of such data (General Data Protection Regulation).

[2] Also see Ishii (2021) and Komukai (2018) for an explanation of the contents of the guidelines [8] [13].

> For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint.
>
> Secondly, Article 20 (1) provides data subjects with the right to transmit personal data from one data controller to another data controller without hindrance.
>
> …
>
> In addition to providing consumer empowerment by preventing *lock-in*, the right to data portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject's control. Data portability can promote the controlled and limited sharing by users of personal data between organisations and thus enrich services and customer experiences. Data portability may facilitate transmission and reuse of personal data concerning users among the various services they are interested in.

As will be described later, all the rights to data portability are discussed as a set with interoperability in the legal systems of each jurisdiction. The guidelines also recommend ensuring the interoperability of data formats in the exercise of the right to data portability[1, p.3].

> As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces (APIs). They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.

A lot of issues have been discussed with regard to the right to data portability since they were established as a right of data subjects in the GDPR. Uga (2018) points out the following issues to be dealt with with regard to the right to data portability: (1) measures to counter identity theft; (2) cyberattacks; (3) disincentivises to invest due to loss of *lock-in*; (4) the burden to comply with data portability; (5) passing on the cost to data subjects; (6)difficulty of defining scope of the right to data portability; (7) all-or-nothing approach to data portability; (8) the jurisdiction; (9) illumining the right to data portability [9, pp.52-61].

The GDPR also stipulates the Right of access by the data subject in Article 15 as a right adjacent to the right to data portability.

The Digital Markets Act (DMA)[3] was proposed by the European Commission on 14 December 2020 as a new business regulation that regulates online platforms in the EU. It proposes to designate the dominant providers in the online platform market as gatekeepers and impose various obligations on them.

The term gatekeeper refers to a provider of core platform services that meets designated criteria. Core platform services include online intermediation services, online search engines, social networking, video sharing platform services, number-independent interpersonal electronic communication services, operating systems, cloud services and advertising services (Article 2 (2)). A core platform service provider will be designated as a gatekeeper by the European Commission if it has a significant impact on the internal market, operates core platform services that are an important gateway for business users to reach end users and has an entrenched and sustainable position in its operations or is predicted to gain such a position in the near future (Article 3 (1)).

The obligations imposed on gatekeepers are defined as those that must be imposed on any gatekeepers and those that may be imposed in addition; in the latter category, the obligation of data portability is stipulated in Article 6 (h). And the obligation of interoperability is stipulated in Article 6 (f).

> Article 6 Obligations for gatekeepers susceptible of being further specified
>
> In respect of each of its core platform services identified pursuant to Article 3 (7), a gatekeeper shall:
> …
> (f) allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services;
> …
> (h) provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access;

Sasaki (2021) notes their similarities to the regulation of dominant operators in the telecommunications market, in that the DMA designates the dominant providers in the online platform market as a gatekeepers, imposes obligations on them and imposes corrective measures or fines if they fail to fulfil those obligations [15, p.Ⅳ-14].

A certain role-sharing can be seen between Article 6 (h) of the DMA and the GDPR with regard to data portability obligations; the GDPR regulates the right to data portability from the perspective of protecting personal information, whereas the DMA aims to do the same from the perspective of regulating business in advance. The latter therefore makes sense as a competition policy.

---

[3] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

1.2 The US

The California Consumer Privacy Act of 2018 (CCPA) is the first comprehensive legislation for the protection of personal information in the US, albeit at the state level. The CCPA came into effect on 1 January 2020 and has provisions similar to the GDPR, establishing the rights of access and portability in Section 1798.100 as one of the rights of consumers.

> Section 798.100
> …
> (d)A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

The Practical Handbook of the Japan External Trade Organisation (JETRO(2019)) positions the right described above as one of consumers' rights to know about personal information that is collected, disclosed and sold [4, p.30].

As a right adjacent to the right to data portability, the CCPA can be read as stipulating a right of access in Section 1798.100 (d), as distinguished from the right to portability. Sections 1798.100 (a) and 1798.110 of the CCPA also stipulate a right to request disclosure.

The California Privacy Rights Act of 2020 (CPRA) amends the CCPA to further strengthen consumer rights. The CPRA was passed by a referendum on 3 November 2020, and is scheduled to come into effect in January 2023. As mentioned above, the CCPA has provisions regarding the right to data portability; the CPRA strengthens right and requires businesses more strict measures.

> Section 1798.130. Notice, Disclosure, Correction and Deletion Requirements
> (a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115 and 1798.125, a business shall, in a form that is reasonably accessible to consumers:
> (3) …
> (B) …
> (iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used machine-readable format that may also be transmitted to another entity at the consumer's

request without hindrance. ‘Specific pieces of information’ do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer’s personal information from one business to another in the context of switching services.

The International Association of Privacy Professionals (IAPP) states that the right to data portability was already included in the CCPA, but the CPRA has modified the requirement[4]. The CPRA also strengthens the right to request disclosure in Section 1798.110, as a right adjacent to the right to data portability.

The Bill of the Consumer Online Privacy Rights Act of 2019 (CORPA) was introduced in the Congress in 2019 and may become the first comprehensive legislation for the protection of personal information in the US at the state level.

(a) RIGHT TO DATA PORTABILITY.—A covered entity, upon the verified request of an individual, shall export the individual’s covered data, except for derived data, without licensing restrictions— (1) in a human-readable format that allows the individual to understand such covered data of the in dividual; and (2) in a structured, interoperable, and machine readable format that includes all covered data or other information that the covered entity collected to the extent feasible.

The US Federal Data Privacy Bill summary of the Consumer Online Privacy Rights Act (COPRA) (JETRO(2021)) positions the right described above as one of individual’s right [5, p.27].

As a right adjacent to the right to data portability, the COPRA can be read as stipulating a right to access and transparency in Section 102, as distinguished from the right to portability.

The Bill of the Augmenting Compatibility and Competition by Enabling Service Switching Act (ACCESS) was introduced in the Congress in 2021.The legislation, when it passes, will regulate data portability obligations from the perspective of regulating business[5].

SEC. 3. PORTABILITY.

---

[4] https://iapp.org/news/a/top-10-operational-impacts-of-the-cpra-part-4-other-expanded-rights-and-obligations/

[5] The bill was proposed as one of five bills on digital platforms, which are: the American Innovation and Choice Online Act, the Platform Competition and Opportunity Act, the Ending Platform Monopolies Act, the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act and the Merger Filing Fee Modernization Act.

(a) IN GENERAL.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including APIs) to enable the secure transfer of data to a user, or with the affirmative consent of a user, to a business user at the direction of a user, in a structured, commonly used and machine-read-able format that complies with the standards issued pursuant to section 6 (c).

SEC. 4. INTEROPERABILITY.

(a) IN GENERAL.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including APIs) to facilitate and maintain interoperability with a competing business or a potential competing business that complies with the standards issued pursuant to section 6 (c).

Prior to the proposal of this bill, the Subcommittee on Antitrust (2020) recommended interoperability and data portability, requiring dominant platforms to make their services compatible with various networks and to make content and information easily portable between them [12, p.20].

1.3 Japan

Japan's Act on the Protection of Personal Information (APPI) was promulgated on 30 May 2003 and came into effect on 1 April 2005. A revision of the APPI was promulgated in 2015, taking into account the necessity of facilitating the proper use of big data, including personal data, and the need to provide a response to the globalisation of business activities. The revised APPI came into effect on 30 May 2017. Subsequently, based on the Every-Three-Year Review provision (Article 12 of the Supplementary Provisions) of the Act, the draft Act to Partially Revise the Act on the Protection of Personal Information (Act No. 44 of 2020) was enacted on 5 June 2020. This was promulgated on 12 June of the same year and is scheduled to come into effect on 1 April 2022. The following is based on the last mentioned revision (which had not come into effect at the time of writing).

Article 28 thereof stipulates the right to request disclosure of information on the principal (i.e., the data subject), and while the revised APPI of 2020 stipulates that this is principally to be conducted via electronic means, it contains no provisions regarding the right to data portability.

Article 28

(1) A principal may demand a personal information handling business operator to disclose retained personal data in which the principal is identified, and such disclosure shall be implemented by providing an electromagnetic record or by any other method specified by the regulations of the Personal Information Protection Commission.

(2) A personal information handling business operator shall, when having received a demand pursuant to the provisions of the preceding paragraph, disclose

retained personal data to a principal without delay pursuant to a method demanded by the principal (or by delivering document(s) in cases where disclosure by the method demanded requires a significant cost or where disclosure by the method demanded is difficult) under the provisions of the preceding paragraph. However, in cases where disclosing such data falls under any of each following item, a whole or part thereof may not be disclosed.
…

Japan also has the Telecommunications Business Act (TBA), which regulates telecommunications operators. However, although digital platforms can be subject to the regulation if they engage in telecommunications as a telecommunications operator, the TBA is not the legislation regarding digital platforms.

In recent years, there has been a series of a new legislation regarding digital platforms in Japan, but all of them have been narrow in their scopes and the obligations that they place on businesses are limited, none of which refer to data portability.

First, the Act on Improving the Transparency and Fairness of Specified Digital Platforms (Specified Digital Platform Act (SDPA)) was enacted in May 2020 and came into effect on 1 February 2021. Secondly, the Act for the Protection of Consumers Who Use Digital Platforms for Transactions (Transactions Digital Platform Act (TDPA)) was enacted on 15 April 2021 and promulgated on 10 May 2021. The SDPA is based on the so-called co-regulation method, which stipulates that the governmental involvement and regulation should be kept to a minimum, premised on voluntary and proactive efforts to improve transparency and fairness implemented by online retail operators and digital platform providers such as app stores. Although the SDPA does stipulate the obligation to disclose information in Article 5 (2), it does not include any data portability obligations [16, p.140]. The TDPA is a new legislation proposed in response to problems that have arisen in digital transaction platforms such as online retail operators, including the distribution of dangerous products via online and difficulties in resolving disputes because the distributor cannot be identified. The TDPA is intended to respond to these issues and to protect consumer's interests. Article 5 of the TDPA establishes the right for consumers to request the disclosure of the seller's information to the extent necessary in cases such as when a consumer makes a claim for damages; it does not, however, include any data portability obligations.

2 Direction of Legislation in Japan

Above, we have looked at the provisions of the GDPR in the EU, the CCPA, the CPRA and the CORPA in the US for the protection of personal data/information regarding the right to data portability. We have also reviewed the right to request disclosure in Japan's APPI, as is a right most adjacent to it for present. Furthermore, in terms of new movements in relation to the obligation of data portability, we have looked into the two proposed regulations on business, the DMA in the EU and the ACCESS in the US, and summarised the situation in Japan. For example, if we want to transfer our webmail data to another company's service, the obligation of data portability in advance

will be imposed on companies on the basis of the DMA in the EU and the ACCESS in the US, and consumers can request data transfer on the basis of GDPR in the EU, CCPA, CRPA and CORPA in the US. On the other hand, the current Japanese legal system only allows for disclosure requests[6]. Let us now consider the direction of legislation in Japan.The following legislation proposals have already been made.

The Personal Information Protection Commission (2019), in its so-called three-year review, stated the following about the introduction of data portability [14, pp.17-18].

> In relation to data portability, voluntary initiatives in the private sector have already been undertaken by Personal Data Trust Bank, and it is welcome that such initiatives are being undertaken on a voluntary basis in line with the APPI. The voluntary implementation of such initiatives in line with the APPI is to be welcomed. On the other hand, the legal obligation of data portability is not only from the perspective of personal data protection, such as the protection of individual rights and interests, but also from the perspective of industrial policy and competition policy. The EU has introduced new provisions in the GDPR to allow the transfer of personal data directly from one controller to another, but only where it is technically feasible to do so. The need for such a provision in Japan is currently being discussed in various areas, including consumer needs, benefits for operators, practical burdens, etc. Therefore, it is necessary to keep a close eye on the progress of these discussions.

Ishii (2021) identifies the following options for legislation on the right to data portability for personal information: (1) establishing provisions similar to the GDPR; (2) establishing provisions to reinforce current efforts centred on Personal Data Trust Bank[7]; (3) expanding the right to request disclosure; (4) legislating in specialised fields such as finance and medical care. On the basis of these options, Ishii argues that as it is easier to implement legislation by enhancing existing provisions than by establishing a new right to data portability, option (3) is the most realistic choice. Ishii also argues that we should consider mechanisms that can enhance competitiveness separately from

---

[6] After leaving the paper, the proposal of the Data Act and the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space was released in the EU. It is reported that the EU is also considering legislation in individual sectors, such as not only healthcare but also automotive, and the issue of data portability in these individual sectors needs to be considered in Japan as well.

[7] Personal Data Trust Bank is the business of managing personal data based on contracts with individuals or other arrangements, and providing data to third parties based on the instructions of individuals or on pre-specified conditions. In accordance with the *Guidelines for Certification of Information Trust Functions ver1.0* formulated by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry, the Japan Federation of IT Organizations has been conducting the Personal Data Trust Bank certification business since the fall of 2018, and has certified five companies as of March 2020 [10, p.234].

considerations on the legal systems relating to personal information protection [8, pp.169-170] [8].

Elsewhere, on 25 June 2021, the Japan Fair Trade Commission (JFTC) and the Competition Policy Research Centre (CPRC) (2021) compiled a *Report of the Study Group on Competition Policy in the Data Market*, which highlighted the importance of ensuring data portability and interoperability. According to the report, specific measures and targets should be considered from the perspective of cost and innovation, in such a way that they do not become a factor that hinders competition. In this regard, the report stated that it will be necessary to carefully consider factors such as the size of business operators, whether the data they hold is industrial data or personal data, and what stage of development the field and markets are in that are to be regulated. The report notes that, especially for digital platforms, ex-post regulations implemented under the existing Antimonopoly Act may not provide a sufficient response and therefore that there may be a need to consider ex-ante regulation as a preferable extra measure. The report also found that it would be beneficial to request various industries to undertake study on a voluntary basis regarding best-practice approaches to formulating regulations on interoperability and data portability and that the government should intervene when necessary [6, pp.58-61].

Legislation in Japan regarding data portability appears to be moving in two directions: the direction envisaged by Ishii (2021), in which the right to data portability is treated as legislation for protection of the personal information, and the direction proposed by the JFTC and CPRC (2021), in which data portability is mandated through legislation on business regulations.

If Japan is to legislate on the right to data portability as for the protection of personal information, it is important to remember that the new legislation on personal data/information in the EU and the US has adopted a new approach, establishing the right to data portability separately from the conventional right to request access/disclosure.

If Japan is to legislate on the obligation of data portability by way of business regulations, it seems that it will also inevitably have to enact a new legislation for digital platforms in some way. As the JFTC and CPRC (2021) report states, it is conceivable to enact data portability legislation as either ex-ante regulation or co-regulation [9]. This could be done by either including data portability regulations as a part of comprehensive legislation on digital platforms, in a manner similar to the DMA in the

[8] Ishii also notes that the OECD (2021) has highlighted that data portability systems focused on data protection do not always promote competition effectively [11, p.168].
For more on the links between the right to request disclosure and the right to data portability as stipulated the current version of the APPI (before its revision in 2020) in Japan, see Itakura (2020) [16].

[9] The report states that "there is value in requesting various industries to undertake study on a voluntary basis regarding best-practice approaches to formulating regulations on interoperability and data portability and that the government should intervene in when necessary". This is interpreted as referring to *co-regulation*.

EU, or through legislation that is specific to data portability, such as the ACCESS in the US. There are those who argue from the legislative perspective for the protection of personal data that the right to data portability is both too broad and strict in that it does not specify services, nor take into account the scale of the businesses and also is applicable uniformly, but it seems worth noting that the DMA in the EU designates core platform services that have a certain (not insignificant) degree of influence in the market as gatekeepers. Although Japan's SDPA and TDPA stipulate certain obligations of information disclosure, their legislative purposes are arguably different from the obligation of data portability. To consider where or how to position rights/obligations relating to data portability in our system, it will not suffice to think only of extending one or some conventional rights or obligations; it will be worthwhile to probe into the desirability of designing a new frame for them as Japan developes a full-fledged digital society.

Interoperability is a dependable companion to data portability; data portability would not be as usable a right without it. They were discussed as a set in the course of legislation both in the EU and the US.

Desirably every one of those issues Uga has set out above[10] may be dealt with in legislation rather than in its application if the right to data portability is to be introduced into Japan.

The GDPR will require data controllers to use formats and templates that are structured, commonly used and machine-readable in order to enable data portability, which could place a significant burden on data controllers. There has also been concern that consumer welfare may in fact be hindered because the right to data portability apply to both small-scale new entrants into the market and to monopolies, which may make it difficult for new entrants from the perspective of competition law, incentivising large, well-funded companies to form oligopolies. Whereas there are some who argue along these lines that the right to data portability is both too broad and strict [9, pp.54-60], others argue that data portability should not be mandatory and should be addressed, where necessary, through the enforcement of competition law [2, p.10]. In this way, data portability has been discussed not only as an issue of legislation for the protection of personal data/infomation, but also as an issue that spans competition policy [7] [9, pp.22-29] [11].

In the midst of implementing various policies aiming at the digital single market, the EU has positioned the protection of personal data as a basic human right based on the Charter of Fundamental Rights of the EU and has used the GDPR to set out not only obligations for businesses but also various rights for data subjects, such as the right to data portability. The GDPR forms an important part of legislation in regulating digital markets in the EU. As we envision images of a convenient future that allows data to be

[10] See p.3.

[11] Uga (2018) and Ishii (2019) highlight the fact that data portability may be discussed under EU competition law in the context of whether it is unlawful to deny access to data held by an operator under Article 102 of the Treaties of the European Union, or in relation to the Essential Facilities Doctrine. Both Uga and Ishii are cautious about applying the Essential Facilities Doctrine in the context of data portability, given the strictness of its requirements.

transferred freely between various services, if we do not make an effort to standardise the format for doing so at a very early stage, individual business operators may proceed with digitisation in their own unique formats. Once this has happened, it will become most difficult to unify those formats. In addition, while it is true that there may be situations where the enclosure of data can be dealt with by enforcing competition law after the fact, by that time it may already be too late to create a competitive environment, as one company may have a monopoly, or several companies may have formed an oligopoly. Thus, enforcement of competition law can only be a remedy after the fact, leaving no room for data portability.

References

1. Article 29 Data Protection Working Party (2017), Guidelines on the right to data portability.
2. Barbara Engels (2016), Data portability among online platforms, Internet Policy Review, Volume 5, Issue 2, p.1.
3. DLA PIPER (2022), DATA PROTECTION LAWS OF THE WORLD, Full Handbook.
4. Japan External Trade Organization (JETRO) (2019), California Consumer Privacy Act (CCPA) Practical Handbook.
5. Japan External Trade Organization (JETRO) (2021), The US Federal Data Privacy Bill summary of the Consumer Online Privacy Rights Act (COPRA).
6. Japan Fair Trade Commission (JFTC) and Competition Policy Research Centre (CPRC) (2021), Report of the Study Group on Competition Policy in the Data Market.
7. Kaori Ishii (2019), Considerations on Peripheral Areas of Privacy and Personal Information Protection Law: Focusing on Intersection with Competition Law, Journal of Information and Communications Policy, Vol. 3, No. 1, IV-1.
8. Kaori Ishii (2021), 'The Right to Data Portability' in Terms of Personal Information, Disclosure & IR, vol. 18, p.168.
9. Katsuya Uga (2018), On the Right to Data Portability, Journal of Consumer Law Research, Vol. 5, p.2.
10. Ministry of Internal Affairs and Communications (2020), 2020 White Paper on Information and Communications, p. 234.
11. OECD (2021), Data portability, interoperability and digital platform competition.
12. Subcommittee on Antitrust(2020), Commercial and Administrative Law of the Committee on the Judiciary, Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations.
13. Taro Komukai (2018), Data Portability, Jurist, Vol. 1521, p.26.
14. The Personal Information Protection Commission (2019), The Act on the Protection of Personal Information: Revision in Every 3 Years – Outline of Framework Amendment.
15. Tsutomu Sasaki (2021), Regulation of the Online Platform Market in Europe and the United States: Dominant Platform Regulation Approaches, Journal of Information and Communications Policy, Vol. 5, No. 1, IV-1.
16. Yoichiro Itakura (2020), Data Portability on Digital Platforms, Current Consumer Law, Vol. 46, p.135.