

Title	Chapter 2-Focus : Data portability : breaking free of the Behemoth?
Sub Title	
Author	Iida, Kyoichi
Publisher	Keio University Global Research Institute
Publication year	2025
Jtitle	Monsterizing Platform Power and Law ; Volume 2. Platforms and Power: How to Tame the Monsters ,p.67- 70
JaLC DOI	10.14991/KO11003002.00000002-0067
Abstract	
Notes	Chapter 2 : The Behemoth as a communication infrastructure
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000002-0067

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

Chapter 2 - Focus

DATA PORTABILITY

: Breaking Free of the Behemoth?

Kyoichi Iida^{*}

1 What is Data Portability?

“Data portability” refers to data such as usage history collected and stored by one service for a specific user (hereinafter referred to as “personal data”) can be reused by other services, therefore, making it portable.

For instance, if you want to use a new music streaming service, data portability would allow you to transfer your playlist from your current service to the new one. This way, you can continue to enjoy your curated playlist of favorite songs without starting over, thus lowering the barriers to switching services. By enabling the transfer of accumulated personal data from one service to another, data portability provides users with more options.

Digital platforms (hereinafter referred to as “DPF(s)”), which possess vast amounts of data and leverage the precision of algorithms and AI, hold power comparable to that of nation states and are likened to the Behemoth in the Old Testament (Tatsuhiko Yamamoto, “Modern Sovereign States and Digital Platforms: Leviathan vs. Behemoth”, in Hajime Yamamoto (ed.), “Basic Theories of Constitutional Law” (Shinzansha Publisher, 2022), pp. 147-181). If a user of DPFs, such as social media or email services, wants to use another DPF, they would not be able to transfer their personal data such as past postings over to another DPF. If so, it must be said that there are certain hurdles to switching DPFs. As a data subject, any user would be able to use another DPF under better conditions compared to a situation where past personal data has not been transferred. Such a situation of switching DPFs (=breaking free from a Behemoth) is a typical situation where data portability is essential.

Data portability is advantageous for users in that it allows to utilize other DPF services more effectively, but it also poses a disadvantage for DPF operators by increasing the possibility of users switching to other DPFs. By enabling access to and transfer of personal data at any time, data portability is expected to improve services and create new value through the effective use and reuse of personal data. However, a potential issue is that making data portability too easy could have serious privacy and cybersecurity implications (Peter Swire, “The Portability and Other Required Transfers Impact Assessment: A Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations” (2022), p. 1).

^{*} **Kyoichi IIDA:** Guest Researcher in Keio University Global Research Institute, Attorney at law.

2 DPFs and Data Portability

In terms of ensuring the initiative of individuals in using their personal data, data portability is a valuable example of the development and diffusion of effective user-centered privacy-enhancing technologies and is regarded as the first tool in the data economy that enables individuals to enjoy the intangible wealth of personal data. The right to transfer personal data to other data managers free of charge is a powerful means of promoting DPF interoperability and enhances individual control over their own data, as it is considered to be a new right concept not present in previous Personal Information Protection Acts, whereby it strengthens the individual's ability to oppose DPF operators and encourages individuals to use data in a way that is controlled by the individuals themselves.

Transferring personal data accumulated by DPFs is often practically difficult, leading to insufficient control over one's own information and therefore undesirable from the perspective of privacy or enhanced involvement of the individual regarding their personal information.

In terms of promoting competition, the introduction of data portability is considered to be driven by concerns about the monopolization of information due to the growing influence of DPF operators, such as GAFAM, who provide the infrastructure for online business and communication. In the modern information society, if there is a lack of data portability, important data from the past can be trapped within specific DPFs, potentially lost because it cannot be taken out, and in an AI society where reality and data are highly inter-linked, this may affect real life in its entirety. Therefore, ensuring the possibility of leaving DPFs is crucial to maintain competition and achieving autonomously correct order.

In other words, data portability has the potential to help resolve the above three issues associated with DPFs. The OECD Digital Economy Papers "Mapping data portability initiatives, opportunities and challenges," published in 2021, acknowledges its importance and necessity, pointing out that "data portability has become an essential tool for enhancing access to and sharing of data across digital services and platforms." Data portability is precisely what enables users to voluntarily liberate themselves from the giant monster Behemoth (DPF).

3 The Right to Data Portability?

The new right enabling data portability is called the "right to data portability" and is established in Article 20 of the General Data Protection Regulation (GDPR). The EU Data Protection Directive has played a fundamental role in the protection of personal data within the EU since 1995. As its replacement, the GDPR came into effect on May 25, 2018. Within the reforms on European data protection legislation, the right to data portability, which facilitates the movement of citizens' personal data to and from service providers, is placed among the fundamental rights of European citizens. The purpose of the right to data portability is to: ① strengthen the right to control personal data and allow individuals to play an active role in the data ecosystem; and ② address the risk of being locked-in to certain Internet-based services and the cost of

switching services even if they are switched, thereby helping to protect personal data. The right to data portability is also expected to encourage innovation by utilizing personal data and improving user convenience through promoting the sharing of personal data under user control.

In order to request a transfer under the right to data portability, the data in question must be ① personal data concerning the user or ② personal data provided by the user. ① would include call records, records of message exchanges between individuals, and so on, while ② would include data actively and intentionally provided by the individual (email address, user name, etc.) as well as observational data provided by the individual through use of the service or device (personal search history, location data, and other data such as pulse rate tracked by a wearable device). By contrast, any personal data created as part of data processing through user classification or profiling, such as user profiles generated from the analysis of raw smart meter data, risk management such as health checkup results and credit evaluations, any personalization or recommendation processes, are all considered “controller-generated” and not subject to the right.

The right to data portability grants these three rights: ① the right to obtain a copy of the personal data provided by the data subject in a structured, publicly available, machine-readable format; ② the right to transfer personal data obtained by the data subject from the data controller to another data controller without being prevented by the original data controller; and ③ the right to transfer personal data to another data controller directly from the data controller where technically feasible. The right to data portability is exercisable for personal data where the lawful basis for the processing is by consent or contract and where the processing is carried out by automated (computerized) means. In contrast, it cannot be exercised with respect to data processed by the public sector. The exercise of the right must not adversely affect the rights and freedoms of others.

4 Discussion on Constitutional Grounds in Japan

In the context of the Constitution of Japan, various perspectives can be considered regarding the constitutional grounds for the right to data portability.

One viewpoint suggests that the right to data portability is a right to utilize one’s own data, stating that “while the right to data portability can be said to have a secondary purpose under competition law, it requires normative justification beyond justification under competition law, and the right to data portability has an independent purpose of controlling one’s own information on personal data (because the right to data portability can only be invoked by living individuals and cannot be used by companies)” (George Shishido , et al., “AI, Society and Law” [Naoto Ikegai] , Yuhikaku Publishing , 2020, p. 69). This perspective leaves room to speculate whether the right to data portability can be justified on the basis of Article 13 of the Constitution, which guarantees the dignity of individuals.

Next, “we live our lives highly dependent on the pervasive digital networks known as DPFs, through which we obtain information such as news, interact with others, trade with others, and manage our health. In the case of digital communities such as DPFs, we have no choice but to move to another community because

we cannot change the rules (algorithms) democratically through autonomous self-governance. So the only option is to move to another community. Thus, in modern society, it is important to practically guarantee movement between digital communities. The right to data portability, which allows one to transport a set of information deposited in one digital community, is important to guarantee the freedom of such movement. There is a view that “free movement between digital communities is as important as the freedom to physically move between cities (freedom of residence and relocation)” (Tatsuhiko Yamamoto, “The Importance of Personal Information Protection Today,” *Urban Affairs*, February 2019 (2019), pp. 47-50). This view is considered to be based on Article 22(1) of the Constitution, which guarantees the freedom of residence and relocation, as the basis for the right to data portability.

Furthermore, “since data is an important factor of production in digital markets, data portability could spur innovation and create new business models if data is made readily and quickly available. Thus, the right to data portability can be seen as a consumer protection right, as it is expected to deter vendor lock-in effects, promote competition among service providers, and encourage the development of privacy-friendly technologies and interoperable data formats.” This view also points out that “the right to interoperability of systems can be understood as an issue of consumer protection and deterrence of unfair competition rather than data protection.” (Katsuya Uga, “Protection and Use of Personal Information” (Yuhikaku Publishing, 2019), pp. 59-60.) This view can be assumed to be based on Article 13 or 25 of the Constitution regarding consumer protection and consumer rights with respect to the right to data portability. (In Canada, the Consumer Privacy Protection Act, which is part of the Digital Charter Implementation Act, 2022, which provides for the right to data portability, is currently under discussion (Kento Yamamoto, “Canada,” in Tatsuhiko Yamamoto et al. “Comparative Law Research on the Personal Data Protection Law in Various Countries,” KGRI Working Paper, 2024). In addition, the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA) in the US provide for data portability rights.)

5 Conclusion

As people become more aware of their rights regarding their own personal data, and the European Health Data Space, a framework for sharing health data in Europe and extends data portability rights beyond the GDPR, is under consideration in Europe, the demand to be able to manage own personal data is expected to increase (and revisions to the Personal Information Protection Law, such as the institutionalization of allowing requests for disclosure through electronic records, is regarded as a promotion of data portability). The establishment of the right to data portability would not only increase user convenience by facilitating the transfer of users’ personal data from DPFs, but would also contribute to promoting competition among DPF operators to secure users, which may lead to increased user benefits. There is focus on future developments as to whether data portability, which allows users to voluntarily free themselves from the Behemoth, will be established as a right in Japan.