Omitted but Not Forgotten: Evaluating the Right to Data Portability in India's Data Protection Regime

Prof. (Dr.) T.R. Subramanya*

Mitike Shrivastava**

Introduction

The digital economy has grown exponentially over the years, and this has facilitated smooth operation and expansion of businesses, especially those that rely largely on data for decision-making. Businesses that store massive amounts of data in their databases allow them to streamline their products and services, ultimately providing them with a competitive edge over other similar businesses in the market. However, this advantage can also act as a barrier to competition, potentially leading to an anti-competitive market as competitors do not have access to such data, and consumers may be discouraged from switching platforms. The right to data portability helps strike a balance between privacy, user autonomy, and fair competition.

Data portability is a right given to data principals or data subjects enabling access to their data and transmitting the same without any hindrance from one data collector to another. It forms a part of a broader spectrum of rights such as the right to access personal information, right to rectify inaccuracies, right to erasure or right to be forgotten. Through free flow of data, it eliminates the possibility of dominant organizations like Google and Meta from monopolizing the market. It is without any doubt that Data Portability provides greater control to users over their personal data but also presents risks of mishandling data, breaches and unauthorized access.

European Union's General Data Protection Regulation (GDPR), one of the most comprehensive data protection frameworks of the world, specifically mentions this right under Article 20. It has two key aspects: the right to receive a copy of the personal data and the right to transfer the same. However, this right is not absolute, it is limited on the grounds of technical feasibility. The Digital Personal Data Protection Act, 2023 of India, which is largely based on the GDPR, initially included data portability as a right for its data principals, however, the same was omitted during the passing of the legislation. This article attempts to identify the possible

* Prof. (Dr.) T.R. Subramanya, Dean, School of Legal Studies, CMR University, Bengaluru

** Ms. Mitike Shrivastava, Research Scholar, School of Legal Studies, CMR University, Bengaluru.

reasons for this exclusion. It further examines the significance of the right and whether excluding the same has any potential impact on the Indian data protection framework. It is worth noting that though right has not been included explicitly, an aspect of it in the form of consent managers has been incorporated. These managers act as a single contact point between data principals and data fiduciaries. In order to understand this decision better, the article explores the evolution and meaning of data portability and the scope and applicability of the right under the GDPR. As India progresses to build a strong, secure digital environment, it becomes inevitable to evaluate its adequacies and inadequacies and whether it impacts India's objectives of safeguarding individual rights and promoting innovation and economic growth.

Understanding data portability

The idea of data portability first emerged in 2007 and was introduced by Brad Fitzpatrick, an American programmer and the founder of LiveJournal. Fitzpatrick proposed the idea to overcome the challenges faced by the users in managing multiple social media accounts. His solution to the same was simple. He suggested creating a system that would enable users to transfer their personal data from one site to another. The idea gained acceptance from major tech companies like Google and Microsoft, however, it quickly lost momentum[1].

Portability re-emerged in 2018 as a viable solution to concerns about dominance and anti-competitive practices by a few major industry players, particularly those in social media industry. In the following year, Facebook's CEO Mark Zuckerberg himself emphasized the need for updated internet regulations in four critical areas: harmful content, election integrity, privacy, and data portability[2]. He highlighted that data portability not only provides users with a choice to handle their data but also enables a healthy competition among developers. As a result, data portability was recognized as a right under European Union's General Data Protection Regulation[3], California Consumer Privacy Act[4] and Singapore's Personal Data Protection Act[5]. The International Organization for Standardization explains data portability as

[1] Gabriel Nicholas, *The New Portability: Designing Portability with Competition in Mind,* Engelberg Ctr. on Innovation L. & Pol'y, N.Y.U. Sch. of L. (May 15, 2024 9:42 PM) https://www.law.nyu.edu/sites/default/files/The_New_Data_Portability.pdf

[2] Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, Wash. Post (April 30 2024 11:45 PM) https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

[3] Regulation 2016/679, art. 20, 2016 O.J. (L 119) 1 (EU).

[4] Cal. Civ. Code §§ 1798.105, 1798.110, 1798.115 (West 2024)

[5] Personal Data Protection Act 2012, No. 26, § 26G (as amended by the Personal Data Protection (Amendment) Act 2020) (Sing.)

the ability to move data between systems without requiring users to manually input the same information again.[6]

At its core, data portability is a right that enables individual internet users to access, copy and export their personal data across digital platforms[7]. It supports a dynamic digital ecosystem in which data subjects can move their data from one controller to another, while safeguarding data's integrity and usability, and without any interference from the original controller[8]. This right enhances individual autonomy over personal data that has been voluntarily provided to a data controller and promotes greater transparency and accountability on part of the controllers[9]. Furthermore, it allows users to make more meaningful use of their data—for example, by comparing services, identifying better deals, or analyzing their spending and consumption patterns.

In order to understand better, the model of Spain can be examined; the Spanish Law provides for a right to content probability which means that the content that the users have posted on their social media accounts can be transferred from one site to another, without the requirement individually repost again[10].

Another example is the midata program of the U.K. government which was launched in 2011. The programme was an initiative by U.K.'s Department for Businesses, Innovation and Skills. It allowed consumers access to their personal data in an easily accessible digital format. In this programme a consumer could download his/her midata file, which contained a record of 12 months of personal current accounts transaction history. The consumer could have this file analysed by a comparison provider. Gocompare.com is an example of one such comparison

---

[6] 3.2.1, ISO/IEC 19941:2017
https://www.iso.org/obp/ui/#iso:std:iso:ts:18101:-1:ed-1:v1:en:term:3.23
[7] Information Commissioner's Office, *Right to Data Portability,* (May 1, 2024, 3:30 PM)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/
[8] Julien Benistant, *Data Portability on Social Networking Sites*, Vrije Universiteit Amsterdam (2023) (May 5, 2024 8:30 PM)
https://ictinstitute.nl/wp-content/uploads/2023/12/Master_Thesis_Data_Portability_SNS_JBenistant_FINAL.pdf
[9] Michiel van Schaijck, *GDPR Top Ten #1: Data Portability Legal obstacle or opportunity?,* Deloitte (May 5, 2024 8:30 PM)
https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-data-portability.html
[10] Jurre Reus, *Data portability in the EU: An obscure data subject right*, Int'l Ass'n of Privacy Professionals (May 07, 2024 7:45 PM)
https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/

provider; these providers offered customised information and assisted in identifying possible account switching options[11].

In the U.S.A. the Obama Administration also launched a My Data initiative in 2010, which aimed to liberalize federal data of various kinds of personal data. Blue Button was introduced for health data while the Green Button was for electric utility Data. Unlike U.K. portability, this initiative was aimed to enhance easy and secure access of data rather than the ability of direct switching of service providers[12].

Right to data portability under GDPR

Working Party, Article 29[13] in its opinion on 'purpose limitation' highlighted the significance of portability. It stated that enabling data portability could help both consumers as well as businesses. It can ensure that a balanced value from big data is derived and used by the business. It observed that such a right could enhance transparency, reduce discriminatory practices, and minimize the risks associated with inaccurate data being used in decision-making processes. Additionally, WP 29 emphasized that data portability should be seen as part of a broader framework that provides data subjects with meaningful mechanisms to access, correct, delete, transfer, and manage user data—either directly or through a third party. These observations and recommendations are reflected in Article 20 GDPR.

Article 20 GDPR provides for the right to data portability, giving individuals an enhanced control over their data. Under Article 20(1), data subjects have a right to receive data concerning them, specifically data they have 'provided' to a controller, in a structured, commonly used, and machine-readable format[14]. This right applies only where the processing is based on consent or on a contract, and the data is processed by automated means[15]. The purpose of this provision is to make it easier for individuals to retrieve their data for their own use or to share it with other service providers. However, the scope of this right is limited to personal data which is specifically provided by the user; not all data that the controller holds

[11]Kaori Ishii. *Discussions on the Right to Data Portability from Legal Perspectives. 13th IFIP International Conference on Human Choice and Computers* (HCC13), 338 (Sep 2018, Poznan, Poland.) (May 07, 2024 7:45 PM)
https://inria.hal.science/hal-02001955/document
[12] *Id.*
[13] Hereinafter WP29.
[14] Regulation 2016/679, art. 20(1), 2016 O.J. (L 119) 1 (EU
[15] *Id.*

can be accessed. For example, users cannot request access to inferred or derived data under this right.

Apart from just receiving their data, individuals can request direct transmission of their data from one controller to another, where such a transfer is technically feasible[16]. The purpose of this sub-clause is to reduce friction at the time of changing service providers and encourages competition by allowing consumers to move their data across platforms without undue hurdles. However, this right is subject to the condition of '*technically feasible'*. It means that such a transfer depends on the ability of both controllers to technically accommodate such transfers, and it does not impose an obligation on the receiving controller to accept the data.

Beyond technical feasibility, Article 20 includes other limitations to safeguard legal and ethical interests. Article 20(3) clarifies that the right to data portability does not override other rights, including the right to erasure under Article 17 GDPR[17]. Further, Article 20(4) specifies that the exercise of this right must not adversely affect the rights and freedoms of others. This includes considerations such as trade secrets, intellectual property, and the privacy of third parties[18]. This provision aims to strike a balance between individual control and autonomy and systemic integrity while respecting technical and legal boundaries.

Portability rights under Article 20 GDPR

Broadly, Article 20 covers two distinct potability rights:

1. Right to receive data: This right is provided to data subjects from the data controller. This is essentially a B2C2B relationship[19]. For example, if a customer uses a particular application to track their physical fitness, they can request this controller to share a report on their exercise patterns to gain an insight in their personal routine and then port the same to another app. It is not necessary that the user in every case transfers the data to another site, they may use the same merely to gain an insight. Article 20(1) grants the right to receive personal data in a *'structured, commonly used and machine-readable format'*, how an individual utilises this data is completely their discretion, they can retain the same for

[16] *Id*. art. 20(2)
[17] *Id* art. 20(3)
[18] *Id*. art 20(4)
[19] Alexandre de Streel, *Making Data Portability More Effective for the Digital Economy,* Ctr. on Regulation in Eur., (May 7 2024 9:45 PM)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866495

their personal use or transfer it further to another controller, this transfer is known as an *indirect transfer*[20].

2. Right to transmit data: This represents a B2B relationship[21]. For instance, a user is currently using a site to track their fitness activities, they come across a new site with better features and wish to use this from now on, the user can request the previous data controller to transfer their data to the new site directly. This method of data transfer is referred to as *direct transfer*[22].

While both rights enhance user control, their enforceability differs in important ways. Even though both the rights allow individuals to enhance control over their data and smooth data movement, the right to transmit is relatively a weaker right. It can be exercised only when it is technically feasible. The feasibility of the transfer is to be decided on a case-to-case basis. Whereas the right to receive is a stronger right which needs to be executed without any hinderance from the controller. Hinderances could result due to unreasonable cost for delivering data, excessive delay, deliberate confusion, and complications in the process[23].

Categories of personal data covered under Article 20 GDPR

The right to data portability under Article 20 applies only to personal data 'provided' by the data subject. This encompasses two main categories. Firstly, it covers data knowingly and willingly given such as name of the user, age, email. Secondly, it extends to observable data such as search history or step counter data etc., this is the category of data that is provided as a result of using the site or service. However, an inferred data which is collected and processed through web tracking devices falls beyond the purview of this right.[24] Additionally, the right applies only to processing that is carried out on the basis of consent or a contract. Data processed under other lawful bases, such as legitimate interest or legal obligation, does not qualify under the category of personal data under this article.

[20] *Supra* note 8.
[21] *Supra* note 17.
[22] Supra note 18.
[23] *Supra* note 17.
[24] *Id.*

Expected data format

For the right to be meaningful, it is essential that the personal data requested is provided in a format that allows re-use and supports interoperability. This means that data should be organized in such a way that it enables it to be transferred across different systems or platforms without requiring substantial modification. The concept of *interoperability* refers to the ability of different systems or organizations to work together effectively by exchanging information in a manner that aligns with shared operational goals[25]. This involves technical compatibility which means that systems should be able to understand and use the data being exchanged.

Recital 68 GDPR clarifies that the right to data portability does not impose a duty on data controllers to modify their technical infrastructure to make it compatible with other systems. In other words, while the data may be presented in a commonly used and machine-readable format, there is no requirement for organizations to adopt uniform software or platforms to facilitate portability. Thus, the ultimate objective of portability is to achieve interoperable system rather than a compatible one[26]. The format may be tailored according to the needs of each sector but it should be interpretable. Formats which require expensive licensing should be avoided, and if there is sector specific format, data shall be provided in an easily accessible and widely acceptable format such as .xml. etc[27].

Exploring the absence of data portability in the Indian data protection framework

In contrast to the detailed provisions on data portability under the GDPR the absence of a comparable right within the Indian data protection regime raises important questions about user autonomy and data mobility, highlighting the need for an examination of this gap and its potential implications.

After extensive deliberations over the years, India enacted a dedicated data protection law in 2023. The long-awaited Data Protection Bill transitioned into a law as 'Digital Personal Data Protection Act, 2023'. This is a significant step by India towards strengthening data privacy

---

[25] *New European Interoperability Framework,* Eur. Comm'n (May 9, 2024 10:00 PM) https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf
[26] *Guidelines on the right to data portability,* Article 29 Data Prot. Working Party,(May 9, 2024, 10:00 PM) https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
[27] *Supra* note 17

and security measures. It introduces various rights for data principals including the rights to access their personal information[28], right to correction and erasure[29] and right of grievance redressal[30]. However, one notable omission from the enacted legislation is the right to data portability. The right was originally included in the 2018 draft of the Data Protection Bill, where the proposed provision was drafted closely to Article 20 GDPR. The provision provided individuals with ability to receive data in a structured, commonly used, and machine-readable format and transfer it from one service provider to another[31]. and also included exceptions to the right, particularly when data processing was linked to state functions, legal obligations, or when the transfer would compromise trade secrets or be technically infeasible[32].

Despite its initial inclusion, the provision was ultimately excluded from the final version of the Act. The rationale behind this exclusion is unclear but there are several aspects that could have contributed to this decision. Nevertheless, several underlying factors may help explain the exclusion. Data portability, while empowering users, also introduces substantial privacy and security challenges. Further, transfer of personal data requires robust technological infrastructure and secure transfer mechanisms, and currently, India's digital ecosystem is still at a developing stage. In the absence of such safeguards, there is a heightened risk of data being lost, altered, or accessed by unauthorized entities during transmission[33]. Even a single incident of unauthorized access can result in identity theft, large-scale data breaches, or financial fraud.

The practical implementation of the right demands a level of digital literacy and operational capacity that is not uniformly available across sectors in India. Concerns over technical feasibility, along with the potential burden on smaller data fiduciaries, further complicate the possibility of introducing this right.

While there are undeniable challenges, the benefits that data portability could offer should not be disregarded. Portability facilitates competition; it promotes competition by limiting barriers imposed by service providers and prevents monopolization of the internet. It can break the lock in patterns and provide equal opportunity to smaller players in the data landscape[34]. A lock-in

---

[28] Digital Personal Data Protection Act, No. 22 of 2023, § 11 (India)
[29] DPDP Act, § 12
[30] DPDP Act § 13
[31] Personal Data Protection Bill, 2018, § 26 (India).
[32] PDP Bill, § 26(2)
[33] Deepa Kharb, *Right To Data Portability: A New Tool To Unlock Digital,* ILI L. Rev., Winter 2020 (May 9, 10:30 PM)
https://ili.ac.in/pdf/dgun.pdf
[34] *Supra* note 14.

situation is when users refrain from switching to another website or service provider because of high switching cost like in case of Microsoft[35].

India's cautious approach may be indicative of its ongoing efforts to build foundational infrastructure for data governance. Introducing data portability prematurely, without ensuring security and standardization, may pose more risks than benefits. However, there are signs that the concept is not entirely off the table. The DPDP Act incorporates a limited version of this right in form of consent managers. Consent managers are entities tasked with the responsibility of enabling individuals to manage their data-sharing preferences through a transparent and interoperable platform[36]. While not equivalent to full data portability, this initiative demonstrates the government's recognition of user agency and its gradual movement toward greater data mobility.

Moreover, in 2025, draft rules which aim to regulate the functioning of consent managers, standardize their technical architecture, ensure interoperability across platforms, and classify data fiduciaries based on parameters such as size, sensitivity of data handled, and sectoral relevance. These developments suggest a willingness on the part of the government to revisit the inclusion of portability as an explicit right once a more secure framework is in place.

In conclusion, although India's current data protection law does not include the right to data portability, ongoing developments like Draft Rules on Consent Managers, setting up the Data Protection Board of India and continued discussions with stakeholders could lead to its future inclusion in line with global standards.

Conclusion

The right of data portability is a blend of user rights, competition, and platform prerogatives, it fosters consumer welfare within the digital ecosystem and mitigates lock-in effects. It also improves market competition in the digital ecosystem and creates opportunities for small businesses and startups. This competition can prevent lock-in situations, improve service quality, lead to technological advancement, and promote economic growth. However, the benefits of this right can only be realized through effective implementation. While technical challenges are relatively easy to identify and rectify, the real challenge lies in policy implementation, government intervention may become necessary in enforcing and ensuring

[35] *Supra* note 11.
[36] DPDP Act, § 7.

compliance, as big organizations have no incentive to voluntarily implement data portability. Further, data portability must be accompanied by stringent security requirements to ensure data protection and reduce possibilities of data breach and unauthorized access.

Data Potability found its place in the initial drafts of Data Protection legislations in India, but subsequently it was excluded from the final draft of the Personal Data Protection Act. It is worth noting that the Act does maintain a limited form of data portability in the form of consent managers and the inclusion of the term 'interoperable platform' in the definition of consent managers suggest that the legislature to some extent intends to ensure this right to its citizens. However, India's infrastructure must first grow and fortify before regulations can effectively be implemented for the same. Without a strong infrastructure and technical safeguards, the possible breaches far outweigh any benefit this right can provide.

In conclusion, for effective implementation of the right of data portability there is a need to stabilize both the technical as well as legal infrastructure. It is essential that the transfer between data controllers takes place seamlessly, as it holds greater importance as compared to transfer of data from a controller to an individual. This requires standardization of protocols that would enhance and promote portability between controllers. Unlike in the European Union, Data Portability is not just a regulatory concern in India but also a technological and infrastructural concern. In order to realize its full potential, efforts from the government are required to address multifaceted issues related to portability. Further public awareness and education about data subject rights are crucial before promoting user autonomy and a culture of data ownership and control. Ultimately, with the right legal framework, data portability has the potential to empower individuals and foster innovation in India's digital economy.