THE RIGHT TO DATA PORTABILITY

Author Information

Name of the Author: Ishita Tulsyan and Pranika Goel

Institution: Research Assistants at Centre for Communication Governance, Students at National Law University Delhi

Year: 4th Year and 5th Year respectively

Contact Information: ishita.tulsyan20@nludelhi.ac.in ; pranika.goel19@nludelhi.ac.in

Acknowledgement

This article has been commissioned for LAWASIA by the Anil Divan Foundation.

1. Introduction

Transitioning from the pre-internet era to a post-pandemic one, one thing that has been evident is the absolute boom in the number of online applications present out there, ready to meet each and every need of the consumer. Even for the same requirement, the user now has the option to choose from a wide range of applications, and often to switch between them. It is this switching between applications, platforms, or other modes of services that data portability deals with.

Clause19 of the Personal Data Protection Bill 2019 stated that the data principal has the right to data portability ("**RtDP**"), but the right is missing from the Digital Personal Data Protection Act.[1] The same right finds mention in various legislations across jurisdictions, including the EU and Brazil, and is proposed in many others like Canada, etc.[2]

However, concerns remain. This paper will explore these concerns and recommend a more suitable approach to incorporating data portability. For this, we must look at Asian in general and particularly India for their specific context and determine whether it should be brought here and if yes, how.

For this, the paper is divided into various parts. *In the first part*, a brief explanation of the right itself is delved into. It looks at why the right was introduced, and what the need for it was. Next, it looks at the many uses of the right. The various jurisdictions that have defined the right are then taken into account and their interpretations of it as per their needs are looked at. To further demystify it, the paper then defines the contours of the right with reference to the various terminologies used in these legislations, with a primary focus on the European Union General Data Protection Regulations or the **EU GDPR**. Thereafter, the interaction of the right to data portability is evaluated in relation to firstly, the many different data rights provided to the users and secondly, the many different fields of law.

In the second part, the main objective is to look at the right from a critical lens. This involves evaluating it over the course of three thresholds - *firstly*, the terminology that it employs in the EU GDPR; *secondly,* if there are any other shortcomings in relation to the impact of having

---

[1] Personal Data Protection Bill, 2019, Bill No. 373 of 2019, 2019 Ind. Legis. Assemb. (India).

[2] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), Article 20 (EU).; Lei Geral de Proteção de Dados (LGPD), Lei No. 13.709, Article 18 (Brasil); *Canada's Digital Charter: Trust in a Digital World, Innovation, Science and Economic Development Canada*, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world (last visited Aug. 31, 2023); Personal Data Protection Bill, 2019, Bill No. 373 of 2019, § 19, 2019 Ind. Legis. Assemb. (India).

such a right; and *thirdly,* if it even seems to serve a meaningful purpose on account of various real-world factors that have an effect on it. In particular, , the Asian perspective comes into the picture in the context of the suitability of the right in this arena. We conclude in this section that the right is useful only so far as it can be employed. For this, the discrepancy between the intent and implementation is explored. Further, based on the Asian context, the role played by factors such as lack of awareness and understanding is taken into account.

In the final part, borrowing from the analysis undertaken in the earlier parts, we put forth suggestions on implementing the right to data portability suitable to the Asian context.

I. Understanding the Right to Data Portability

This chapter introduces the Right to Data Portability and traces it from the very beginning. It aims to understand the terms of the right in the EU GDPR and the impact that they seek to produce. Further, it goes on to trace the interaction of RtDP with other rights, possible overlaps with other fields of laws, and the discussion about it in the academic fora, to open the door for its critical analysis.

(i) History

The exact origins of the RtDP while unclear, started as a discourse unrelated to data privacy and was a technological measure. One of the earliest of these was The Data Portability Project from 2007.[3] This was followed by the internet giants like Facebook and Google.[4]

The history of the RtDP in a data protection regime, however, is the same as that of the EU GDPR. Its predecessor, the Data Protection Directive of 1995 did not envision a right to data portability. EU GDPR was the main document to have first envisaged the right in its initial version in 2012.[5] The current Act was however conceived after a series of changes throughout the time. When it was introduced, the right to data portability by the EU Commission, it read as providing two rights to the individuals - first that a copy of the electronically processed personal data present in a "structured and commonly used format" can be accessed by the users

[3] Barbara Van der Auwermeulen, *How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations,* 33 (57) COMPUTER L. & SECURITY REV. 57, 58 (2016).

[4] Helena Ursic, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, 15 SCRIPTED: A J. L. TECH. & SOC. 1 (2018).

[5] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012.

and second that the said data could be transmitted from one provider to the other. This implied that the way that the data was processed was key to whether it could be portable or not.[6]

This issue was also recognised by the EU Commission and the final text seemed to deal with it. Subsequently, various jurisdictions other than the EU also have either formulated a law that includes the right to data portability in their frameworks or has at least envisioned it in future frameworks.

(ii) Meaning of the right

Article 20 of the GDPR introduces two fundamental principles regarding data portability. Firstly, following a user's request for the right to data portability (RtDP), individuals are entitled to "receive" their data in a format that is structured, commonly used, and machine-readable. This format empowers them to transfer (either in whole or in part) their data to another service. Secondly, if technically feasible, organizations must directly transmit personal data to another service as per the user's request. The provision aims to ensure smooth and seamless data portability while granting individuals greater control over their personal information. Thus, while the first part allows for the flow of data to be B2C2B, the second part facilitates a B2B approach.

To further understand the scope and terms of the right, one must look at the interpretive guidelines of the working party.[7] As per these guidelines, the kind of data that can be called personal data for the purposes of this right would be under a broad definition. *Firstly*, it has to be personal, but that does not discount the pseudonymized data that is linkable to the data subject. Meanwhile, anonymized data is beyond the scope of data portability. *Secondly*, the data would be the one that the user provides. Within this too, there can be three subcategories - data provided by the user explicitly, data gathered upon user observation, and information inferred. It is only the first two sub-categories that can be ported. *Thirdly*, the data provided should “not adversely affect the rights and freedoms of others”. Naturally, with the data provided about the data subject by the data subject, there is also a bunch of data that overlap with third persons, and porting them with the data subject’s data would amount to the nonconsensual transfer of that data for the third parties. This would be against the rights of the said third person. It is to avoid this mishap that if there is any risk of an “adverse” effect on the

[6] Bart Custers & Helena Uršič, *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection*, 6 INT'L DATA PRIVACY L. 4 (2016), https://doi.org/10.1093/idpl/ipv028.

[7] Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 (2016), p. 10 (EC).

rights of the third party, that data may not be ported. Thus, processing of their data is permissible only when it exclusively remains under the data subject's control for purely personal reasons. Further, the entity to whom the data would be ported shall not be permitted to use the associated data of the third person to further its own purposes. However, one important aspect to note here is that the term "adversely" has not been defined or explained apart from a few illustrations in the Working Party Guidelines, and so it remains to be seen where the line would be drawn and how these protections would actually play out.

In case the data controller doesn't oblige to the user's request for portability, there are various grievance redressal mechanisms as detailed in Chapter 4 of the document as well. Various authorities, starting from a supervisory authority to a controller or processor can be accessed for this purpose. Furthermore, under articles 78 and 79, there is also a right to effective judicial remedy in case either of these measures do not work out. Furthermore, there are provisions for compensation that a user can opt for if they suffer any damage as a result of the infringement of the GDPR.[8]

The GDPR does not alone govern this right as lately even the Data Act and DMA have broadened the scope of RtDP.[9] As per Articles 4 and 5 of the Data Act, the user has the right to access and use the "data generated by the products or related services" and the "right to share data with the third parties".[10] Together these are terms similar to the right to access and right to data portability as provided in the EU GDPR. While the GDPR limits the portability right to the data provided by the user, personal data, consent-based data, and data that is processed by automated means, the Data Act expands this limitation and allows for the access and portability of both personal and non-personal data, and allows its access by both the user or anyone on their behalf, which may include businesses.[11]

Meanwhile, in Article 6 (9)(10) of the DMA as well the right of data portability is present, where Business Users have the right to data portability as well.[12] There remain doubts as to how the three legislations interact with each other since the GDPR mandates the data provided

[8] General Data Protection Regulation, art. 82, 2016 O.J. (L 119) 1.

[9] Kranz, J., Kuebler-Wachendorff, S., Syrmoudis, E. et al., *Data Portability*, BUS. INF. SYST. ENG. (2023), https://doi.org/10.1007/s12599-023-00815-w.

[10] EU Data Act, art. 4, 5.

[11] Data Act - Questions and Answers, European Commission https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114

[12] Digital Markets Act, art. 6, ¶¶ 9, 10.

to be in a "structured, commonly used and machine-readable format" while the other two legislations do not impose such restrictions over the data controller, although these legislations are still supposed to be in line with the GDPR. Instead, the Data Act introduces the FRAND terms of fairness, reasonability, and non-discrimination in applying the right to data portability, something that would generally be expected under rule of law, does not directly appear in the text of the EU GDPR.

Meanwhile, another framework that needs to be addressed is the Digital Content Directive, Omnibus Directive, and Free Flow of Data Regulation.

The DCD (Data Control Directive)'s principal goal is to provide customers with the right to access and recover their non-personal data, and so contrary to the GDPR, the DCD does not immediately permit data transfer between two traders. Nonetheless, the primary goal of the DCD is to allow customers to access their data and then share it with other dealers. This new right allows customers to transfer content between providers more easily since it resolves difficulties such as legal, technological, and practical restrictions that previously hampered their ability to retrieve any data collected or generated via their usage of digital material.

(iii) <u>The objectives and advantages of RtDP</u>

Article 1 of the GDPR explains that the objective of the legislation is to protect the "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[13] Thereby, reading the legislation in the context of its main purpose, the main objective of a right to data portability is to enable the data subject to exercise a degree of control over their own data. This is to ensure that there is a healthy balance maintained in the power dynamics of the subject and controller.[14] Thus, as per Article 1, the EU GDPR is primarily a human rights text, and not moulded from the lens of competitiveness.

While these are the legislative objectives of the RtDP, there are various advantages of it that have been debated in academia.

One, it has been deemed key to the functions of increasing market competitiveness and innovation. Even the working party guidelines look at a couple of experimental applications in Europe to conclude that the opportunities for innovation are widened through this.

[13] General Data Protection Regulation, art. 1, 2016 O.J. (L 119) 1.

[14] Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 (2016), p. 10 (EC).

Two, it provides for consumer empowerment by keeping the system from "locking in" the consumer. What this essentially means is that the lack of RtDP is a factor in preventing the consumer from shifting to other service providers of a similar nature, since the user would have to fill in the details of their data again.

Three, RtDP has a role even in the promotion of economic and social benefits. Each time a service provider undertakes the seeking of information from the user, and each time the user feeds in the data, there is a generation of big data. RtDP here promotes the reusing of such data by different platforms.[15] This in turn could also be beneficial for even the environment, but such an advantage will have to be assessed.

(iv) Interaction with the other rights

Right to Access

While the right to data portability attempts to encourage technical re-use of data and minimize user lock-in, the right to data access strives to empower the data subject by allowing him to understand what is done with his data in practice. Furthermore, the scope of those different rights varies: While the right to data portability under the GDPR only applies to personal data provided by the data subject, the right to data access encompasses all personal data.[16]

Intellectual Property Rights

The data when ported is reproduced and distributed. This is something that can cause an infringement of someone else's rights when the request for some IP-protected data is made. However, since the GDPR focuses primarily on user-provided data, the probability of the IP rights of a third party being infringed is quite low, especially when the terms of portability restriction are interpreted narrowly. However, in taking observed data or inferred data as a part of the data ported, there may be cases where the say trade secret or copyright of the data controller itself is at risk. The GDPR guidelines give preference to data portability over the intellectual property rights and state that the IPR cannot be the sole reason to deny a portability request. Meanwhile, this interrelation is much more elaborate when it comes to the Data Act.

After users share information protected by copyright or intellectual property rights on digital platforms, such as images or videos, problems emerge regarding what happens to the licences

[15] Bart Custers & Helena Uršič, *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection,* 6 INT'L DATA PRIVACY L. 4 (2016), https://doi.org/10.1093/idpl/ipv028.

[16] Alexandre de Streel, Jan Kraemer, & Pierre Senellart, *Making Data Portability More Effective for the Digital Economy,* (June 14, 2021).

after they stop using the site. The first consideration is whether the platform and users will be able to utilise the material after the customer has left. The second issue concerns users reusing their material on other sites, which may be in violation of the licenses provided. Further, there needs to be clear cut jurisprudence on how far the concerns of interoperability can be used to justify the use of copyrighted material under fair dealing.[17] These are difficult concerns that must be interpreted in accordance with national legislation. That is also as the DCD allows for portability in IoT aspects as well.[18]

Right to be forgotten/erasure

Data portability does not automatically mean that the data will be deleted from the systems of the organization holding it, nor does it change how long the data will be retained. To enforce any removal of data, the user must enforce their right to erasure, or right to oppose data processing, which are other rights under the GDPR and contrary to the general misconception, are not a part of data portability's function itself. Conversely, if someone wants their data to be deleted, the organization cannot use data portability as an excuse to delay or refuse the deletion request.[19]

(v) Interaction with the other domains

One, the aspects of interoperability and RtDP are closely related while being quite different at the same time.[20] When looked at individually, these are two different concepts, where interoperability is the possibility of two or more platforms, interfaces, or similar other structures to work with other such structures, through models such as horizontal or vertical interoperability. Meanwhile, the two are also deeply interconnected in the sense that to ensure the proper use of the data that is sought to be ported between one application and the other, there needs to be a degree of interoperability between the two platforms.[21] In an interoperable

[17] Copyright Act 1957, Article 52(1)(ab), (India)

[18] Simon Geiregat, *Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive*, 71 GRUR INT'L 495 (June 2022), https://doi.org/10.1093/grurint/ikac042; Simon Geiregat, *Data Portability Rights versus IP – Part II*, KLUWER COPYRIGHT BLOG (2022), https://web.archive.org/web/20230327035931/https://copyrightblog.kluweriplaw.com/2022/09/29/data-portability-rights-versus-ip-part-ii/ (last visited [August 31, 2023]).

[19] Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 (2016), p. 10 (EC).

[20] Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 COMPUTER L. & SECURITY REV. 193 (2018), https://doi.org/10.1016/j.clsr.2017.10.003.

[21] OECD (2021), *Data Portability, Interoperability and Digital Platform Competition,* OECD COMPETITION COMMITTEE DISCUSSION PAPER, http://oe.cd/dpic.

structure, the RtDP has been said to have the potential to facilitate movement and competition. However, there are multiple factors to address in determining the impact of portability and interoperability, and proper market data research is required into it before concluding on its pro-innovation effect.[22]

Two, and connected to interoperability itself as well, the right to data portability features as quite an important aspect of digital public infrastructures. Digital public infrastructure is a system that streamlines people, money, and information to eventually create an ecosystem of goods and service flow.[23] It is this third aspect of the digital public infrastructure that deals with the seamless flow of information that requires a good operation of interoperability to function well between different service providers. The right to data portability, while not directly associated with this, adds to this possibility by supporting ease of change in the said infrastructure.

Three, and the most talked about domain that the right interacts with is competition law. Data being a non-rivalrous resource can be used by multiple entities at the same time. Thus, when portability allows for the easy movement of data from the controller to either the user or another controller upon the user's consent, the monopoly of data is broken, and hence competition is facilitated.[24] This is something that competition law presently also already governs in the form of action against anticompetitive behaviour. However, in exploring the interface between the two, the connection also has to be looked at in the terms of the scope that each covers. While data portability as in the EU GDPR covers personal data and data provided by the user only, competition law does not differentiate between kinds of data and regulates it all in the same manner. What this implies is that while there is initial thrust to the competition provided by the entry of user-facilitated data sharing, the overall change is not anticipated to be much, since a broader scope of the same is already implemented in this sector.

[22] Interoperability & Data Portability, Asia Business Law Journal, https://law.asia/interoperability-data-portability/ (last visited August 31, 2023).

[23] Digital Public Infrastructure: Lessons from India, Observer Research Foundation, https://www.orfonline.org/research/digital-public-infrastructure-lessons-from-india/ (last visited August 31, 2023).

[24] The Impact of Data Portability on Platform Competition, Competition Policy International, https://www.competitionpolicyinternational.com/the-impact-of-data-portability-on-platform-competition/ (last visited August 31, 2023).

In fact, it is feared that a wide implementation of the RtDP would actually thwart competition.[25] This is because the right does not differentiate between services and platforms on the basis of the sizes, and thus, has the potential to be disproportionately heavier on the smaller or newer services, especially when the incumbent service provider is dominant and valuable enough.[26] Further, in the case of a wide implementation, since all platforms could have easy access to the same set of data, any innovation in data processing could also be diminished, thereby also affecting competition.

Four, flowing from the interface between competition law and data portability is the interface between consumer law and data portability. If it is to be accepted that RtDP increases the competition in the market, it can be argued that the result would be a greater variety of choices present with the consumers. This especially considering how the right to choose between different goods and services at competitive prices is one of the essential consumer rights, [27] and thereby is a force of increasing consumer empowerment.

Furthermore, one of the main purposes cited to have the RtDP is to prevent consumer lock-in.[28] While this cannot be called the sole reason for consumer lock-in, its absence certainly contributes in it, since a lack of data portability right results in the raising of switching costs and favouring of incumbent vendors.[29] Meanwhile, it has also been indicated that the presence of consumer empowerment increases the competition in the market and has a positive effect on sustainable growth.[30] However, despite these, formulation of a definite response towards the interrelation of consumer empowerment, market competition and the RtDP would require an in depth study into consumer behaviour in this aspect, something that perhaps should be taken up before the formulation of a data portability regulation.

---

[25] Deepa Kharb and Gunjan Malhotra Ahuja, *Right To Data Portability: A New Tool To Unlock Digital Competition?*, ILI LAW REVIEW WINTER ISSUE (2020) https://ili.ac.in/pdf/dgun.pdf (last visited August 31, 2023).

[26] Lam, W. M. W., & Liu, X., *Does Data Portability Facilitate Entry?,* 69 INT'L J. INDUS. ORG. 102564, (2020) https://doi.org/10.1016/j.ijindorg.2019.102564.

[27] Consumer Rights, Consumer Affairs Division, Ministry of Consumer Affairs, Food & Public Distribution, Government of India, https://consumeraffairs.nic.in/organisation-and-units/division/consumer-protection-unit/consumer-rights (last visited August 31, 2023).

[28] Kuebler-Wachendorff, S., Luzsa, R., Kranz, J. et al., *The Right to Data Portability: Conception, Status Quo, and Future Directions*, 44 INFORMATIK SPEKTRUM 264 (2021), https://doi.org/10.1007/s00287-021-01372-w.

[29] Beatriz Kira et al., *Regulating Digital Ecosystems: Bridging the Gap Between Competition Policy and Data Protection,* 30 INDUS. & CORP. CHANGE 1337 (2021), https://doi.org/10.1093/icc/dtab053.

[30] Huanhui Chen, Chan Lyu, Yao Pan, Zenan Yu, Atlantis Press, *Advances in Social Science, Education and Humanities Research,* VOL. 523 Consumer Empowerment, Market Competition and Sustainable Growth of Enterprises.

2. Critically Analysing the Right to Data Portability

Borrowing from the above detailed discussion on the right to data portability, its origins and its objectives, this chapter goes into the nuances of the right with an aim to critically analyse it. Not only is the phraseology of the right as appearing in the EU GDPR ambiguous and confusing, the right opens up many related questions of privacy and data security. Additionally, the on-ground implementation and even the overall instrumentality of the right have been questioned. We analyse each set of issues in the form of three separate sections.

II.Contentious Phraseology

Essentially, Article 20 of the EU GDPR grants a data subject the right to either receive or request to be directly transmitted any *personal data provided by them* to a data controller in a '*structured, commonly used and machine-readable format*', provided the data is processed using automated means *with consent or under a contract*. Direct transmissions between data controllers would be obligatory only where *technically feasible*. While the right seemingly provides control over one's own data, the import of certain words, phrases and clauses used in Article 20 (or lack thereof) may have the effect of undermining the very objective of the right.

One, the scope of the right is restricted to personal data provided by a data subject. Personal data refers to such information that can be linked to an individual.[31] However, the distinction between personal and non-personal information becomes illusory in practice, for instance, for mixed data sets. Anonymization is said to turn data non-personal. However, studies[32] have illustrated the possibility of re-identifying persons from such anonymized data. How the GDPR right fares in such situations is unclear.

Now there are three approaches to interpreting the term 'data provided by data subject'. Under the narrower approach, only raw data furnished by a user would be subject to portability. While the broader approach espouses that even data collected through observation of user behaviour is covered within the right.[33] Here, an ambiguity arises at the first instance since the GDPR itself does not provide clarity on the matter. While the latter approach is more in consonance

[31] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), Article 4(1) (EU).

[32] L. Rocher Et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 NATURE COMMUNICATIONS 1, (2019); M. Finck and F. Pallas, *They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data under the GDPR*, 10 INTERNATIONAL DATA PRIVACY LAW 11 (2020).

[33] De Hert P. Et al., *The Right To Data Portability In The GDPR: Towards User-Centric Interoperability Of Digital Services*, 34(2) COMPUT. LAW SECUR. REV. 193 (2018).

with the objective of the right in providing greater data controllership, and is a widely accepted interpretation,[34] lack of clarity opens a window for denial of the right's legitimate exercise.

However, generated or inferred data, which is processed based on such raw and observed through machine learning, is outside the ambit of the right, since it is not as such "provided" by the user. Yet a large portion of the data as well as high value data is such inferred data, which remains immune to the right.[35] Furthermore, the rationale for excluding such data (namely, the processed data being the property of the data controller who processed it, based on the fact that the cost of services they provide is the respective raw data) is defeated when we consider such services for which the user pays separately, in which case any data processed from the additional data the latter provides must also belong to such user. [36] Such refined analysis is missing in the right as it currently stands.

Two, the data must be provided on consent or under a contract. This is a corollary of the requirement for the data to be provided by the user. Consider the situation where a user wilfully availing the services of a data controller. In providing such services, the latter also collects certain data for which the user either has not given consent or is not aware of its recording by the controller, essentially observed data. Now the first proviso to Article 20.1 would make such data not amenable to portability, if interpreted in a restrictive sense. However, no clarification is allowed by the GDPR. Further, data received under a legal obligation or upon the direction of statutory authorities would also not be subject to portability.

Three, the data controller is said to be in compliance with the right when a portability request is responded to with the requisitioned data in a 'structured, commonly used and machine-readable format'. Considering that the objective of interoperability can only be attained given these minimum criteria are met, they must be defined unequivocally. Yet, of the three terms, only 'machine-readable' has been defined by the European Union.[37] Thus, reliance must be

---

[34] *Right to Data Portability*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/#ib4.

[35] S Wachter and B Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 Columbia Business Law Review 494 (2018).

[36] FREDERIKE ZUFALLE AND RAPHAEL ZINGG, DATA PORTABILITY IN A DATA-DRIVEN WORLD IN ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW (Cambridge University Press 2021), https://www.cambridge.org/core/books/artificial-intelligence-and-international-economic-law/data-portability-in-a-datadriven-world/F445EC4A9E9665A05E773A88E8840027.

[37] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance, 2013 O.J. (L 175/1), Rec. 21, Reg. 2.

placed on external documents such as the 'Open Data Handbook'[38], published by Open Knowledge International. In fact, the GDPR does not require the format to be interoperable, and only encourages the data controllers to do so under Recital 68. This only half-heartedly operationalizes the intent of the right.

Four, technical feasibility is a defence to refusing a request for direct data transfers between data controllers. The lack of a standard places the smaller data controllers at a special disadvantage as opposed to significant ones like Facebook and Google, since the former utilize third-party software.[39] In fact, absent interoperability (refer to the paragraph above), such technical feasibility would naturally be lacking. In fact, studies have found that the missing infrastructure contributes to a virtually non-existent direct data portability right.[40] This adds to switching cost for the data subjects since they would have to act as the intermediary in such data transfers at their own expense.

Five, the GDPR does not provide any format or manner of making a data portability request. Further complications arise as a request may be made to any part of the data controller's organization or to any employee of such organization. This makes identification of portability requests as well as their compliance onerous for the data controller, and leaves data subjects to fend for themselves.

A dissection of the wording of GDPR leaves us with a host of questions as to the scope and import of the right to data portability. Any legal document granting a data portability right must thus endeavour to account for such shortcomings.

II. **Associated Shortcomings**

Not only does the content of the right to data portability raise concerns, but there are several related issues that arise when we consider the right in consonance with other aspects of a digital economy.

One, the data sought to be ported may not only contain personal information regarding the data subject seeking portability, but also information relating to others. Examples include contact

---

[38] DANIEL DEITRICH ET AL., OPEN DATA HANDBOOK (Open Knowledge International), http://opendatahandbook.org/.

[39] Ruth Janal, *Data Portability - A Tale of Two Concepts*, 8 JIPITEC 59 (2017), https://www.jipitec.eu/issues/jipitec-8-1-2017/4532/JIPITEC_8_1_2017_Janal.pdf.

[40] Sophie Kuebler-Wachendorff Et al., *The Right to Data Portability: conception, status quo, and future directions*, 44 INFORMATIK SPEKTRUM 264 (2021), https://link.springer.com/article/10.1007/s00287-021-01372-w.

lists and group photographs.[41] Such other person may not have consented to allowing a different data controller access to their data. Thus, data portability poses a real threat to privacy of third parties. Article 20.4 of the GDPR provides a way out in the form of the third exception to the right which says that the right shall not be exercisable when it adversely affects the rights and freedoms of persons other than the data subject requesting portability.

However, guidance is lacking on how this exception is to be implemented. Denying portability requests on that basis altogether is too strict an approach given that most data would be in a matrix form. Similarly, allowing portability only when the concerned data is utilized by the new controller solely for the personal purposes of the requesting data subject,[42] diminishes the scope of the right considerably.

Another approach is to only allow portability of the data that the requesting user owns.[43] However, property in the data may reside in different persons and further data protection laws are independent of ownership of the data.[44] Hence, ownership does not offer a viable solution. The solution possibly resides in a balancing act that considers multiple facts such as whether the requesting user has provided the data in question, whether such data as classified as the personal information of another and the level of its sensitivity.[45] Yet, how this balancing is to be undertaken and what factors will gain precedence is something that requires more guidance from policymakers.

Privacy issues also reveal a conflict between other data protection obligations of data controllers and that under the right to data portability. For instance, generally, data controllers have an obligation to ensure protection of privacy in the process of data transfers.[46] However, under the right to data portability, the transferring data controller is absolved of the responsibility for privacy breaches on the transferee's end. The rationale is stated as the choice

---

[41] Ruth Janal, *Data Portability - A Tale of Two Concepts*, 8 JIPITEC 59 (2017), https://www.jipitec.eu/issues/jipitec-8-1-2017/4532/JIPITEC_8_1_2017_Janal.pdf.

[42] Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 (2016), p. 10 (EC).

[43] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 373 (2013).

[44] Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy, SWD (2017) 2 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002.

[45] Erin Egan, *Data Portability and Privacy*, FACEBOOK (2019), https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

[46] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), Article 24, 32 (EU).

of recipient lying with the data subject instead of the data controller as in the former case.[47] This places disproportionate burden on the data subject, requiring them to ensure their privacy in a transfer effected by others. Instead, the transferring controller must ensure that data transfer is occurring through a secure channel to prevent breaches during direct portability.

Two, data security breaches might occur in the process of data portability. This may happen either when a poser of the data subject requests portability, thus gaining access to the personal information of another, or when data is stolen in transmission. This is exacerbated by the absence of standards, including how a portability request may be made and what data is to be transferred and how.[48]

Three, there is no obligation upon the data controller to ensure the quality and accuracy of the data being transferred.[49] While it exists as a separate requirement as a principle for processing of personal information,[50] it does not extend to cover ported data. In a way, the omission makes sense since the ported data is "provided by the data subject". But the justification seems errant in situations where the data is not explicitly given by the user but is collected by observation or otherwise by the controller. At the same time, responsibility on the transferring controller in the regard is warranted since the receiving controller may not have the means to discharge the same.

Practically, the right also poses semantic and syntactic difficulties. The former is illustrated in a situation where the same word may have two equally possible meanings and the latter is exemplified in different forms of data, including integers and strings.[51]

Four, there exists a silent conflict between the right to data portability and Intellectual Property Rights, most specifically delineated by the requirement that the right must not adversely affect third-party rights and freedoms. This limitation provides grounds for denial of a portability request for the reason that it leads to disclosure of the data controller's intellectual property or

---

[47] Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 (2016), pp. 6, 19 (EC).

[48] Erin Egan, *Data Portability and Privacy*, FACEBOOK (2019), p. 2, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

[49] *Right to Data Portability*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/#ib4.

[50] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), Article 5(d) (EU).

[51] Ambika Choudhury, *Understanding the Right to Data Portability, its Limitations, and Benefits*, ANALYTICS INDIA MAGAZINE (22 June 2019), https://analyticsindiamag.com/understanding-the-right-to-data-portability-its-limitations-and-benefits/.

trade secrets in so far as a competing data controller can reverse engineer based upon the data ported.[52]

And five, the ambiguities and grey areas that the right creates provides scope to not only courts and data protection authorities, but also data controllers in interpreting the wording of Article 20 in a host of ways, potentially allowing a convenient interpretation. In practice, instead of doing so individually, data controllers partake in voluntary regulatory schemes.[53] While such schemes are not legally binding per se, opting into one entails similar features of regulation including prescription of norms, monitoring of compliance and correction of deviations.[54] Essentially, this leads to private regulation by non-governmental actors. While private regulation is not altogether harmful, giving such broad powers to non-state bodies invites risks of an unbalanced approach, inevitably harming the unrepresented data principal.

While this complements state regulation, it carries with it the dangers of monopolisation, with the smaller regulatory as well as data controller firms being sidelined. For instance, the Data Transfer Project, being settled by the technology giants by the likes of Apple, Facebook and Google,[55] may impose onerous standards upon smaller controllers, concentrating power in the hands of a few. Further, given the lack of compatibility of standards among these private actors, the lowest among them shall emerge as the denominator, lowering the quality of the right.[56]

Therefore, the right to data portability requires a holistic and interdisciplinary approach to be effective.

III. Is the Right to Data Portability Serving any Purpose?

The semantic and interdisciplinary nuances of the right to data portability aside, the actual implementation and effectiveness of the right are the most important parameters on which to

[52] I. Graef, M. Husovec & N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, 19(6) GERMAN LAW JOURNAL 1359 (2018), 1374-1375.

[53] Examples include the Qiy Scheme settled by the non-profit foundation, Qiy Foundation.

[54] Matteo Nebbai, *Intermediaries Do Matter: Voluntary Standards and the Right to Data Portability*, 11(2) INTERNET POLICY REVIEW (2022), https://policyreview.info/articles/analysis/intermediaries-do-matter-voluntary-standards-and-right-data-portability.

[55] Data Transfer Initiative, https://dtinit.org/.

[56] O.E.C.D., *OECD Expert Workshop on enhanced access to data: Reconciling risks and benefits of data re-use* Technical Report, DANISH BUSINESS AUTHORITY (2014), https://www.oecd.org/sti/ieconomy/expert-workshop-enhanced-access-to-data-reconciling-risks-and-benefits-of-data-re-use.htm.

judge the quality of it. And research (as discussed below) suggests that the right does not prove to be at par on that touchstone.

One, the level of awareness about the existence of the right and knowledge on how and when to exercise it is largely lacking. [57] Apparently, RtDP is the right least known to data subjects in the EU, only about 30% of the sample being at least aware of its existence. This is in stark contrast to the other GDPR rights, which enjoy awareness among more than 50% of the population. In fact, RtDP is hailed as the least understood right, judged as difficult to comprehend its import. Interestingly, the need for the right is real since it ideally operationalises the possibility of switching between service providers by making the process of porting data simple and safeguarding the transferred data in the process.

Two, direct data portability, that is direct transfer of user data between data controllers, is said to be an illusory right on account of the fact that the necessary infrastructure is lacking.[58] Even indirect portability is not properly implemented with shortfalls in compliance with the prescribed timeline, data format as being "structured, commonly used and machine-readable", and the broader interpretation of the nature of data covered by the right. Further, data import features at the receiving data controllers, that allow the data subject to upload the ported data at the new controller's platform, are not satisfactorily available.[59]

Three, as a function of the aforementioned points, the right is rarely exercised by data subjects. It is even less enforced and adjudicated, thus stripping it off the opportunity to develop. Such is the case even in large data economies, including the European countries.[60] So the usefulness of the right is quite in contrast with its propounded advantages.

Even Data Protection Authority discussions on the right have been far and sparse, limited to what kind of services may be subject to portability of data.[61] But there are no judicial or

---

[57] Sideri M. & Gritzalis S., *Are We Really Informed on the Rights GDPR Guarantees?*, Paper presented at the International Symposium on Human Aspects of Information Security and Assurance (2020).

[58] Sophie Kuebler-Wachendorff Et al., *The Right to Data Portability: conception, status quo, and future directions*, 44 INFORMATIK SPEKTRUM 264 (2021), https://link.springer.com/article/10.1007/s00287-021-01372-w.

[59] E. Syrmoudis Et al., *Data Portability Between Online Services: An Empirical Analysis On The Effectiveness Of GDPR Art. 20*, 3 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 351 (2021).

[60] Jurre Reus and Nicole Bilderbeek, *Data Portability in the EU: An Obscure Data Subject Right*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (24 March 2022), https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/#.

[61] See: Dutch Data Protection Authority at https://autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-dataportabiliteit; Lithuanian Data Protection Authority https://vdai.lrv.lt/uploads/vdai/documents/files/01%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gair

administrative pronouncements discussing the semantic and application issues of the right, except the two Dutch cases where drivers requisitioned data from taxi aggregator apps, that upheld the right while noting that the requirement of providing data in a machine readable format does not mandate the use of a CSV or API format over a PDF.[62]

Hence, implementation of the right is inadequate, demonstrating a wide abyss between the intention of the GDPR drafters and data protection authorities and the real-world application of the right to data portability.

IV. The Asian Perspective

Given the background of the right to data portability in the GDPR, an essential question that arises is with respect to the unique challenges to the framing and implementation of the right that may arise specifically in the Asian economies. Comprising of data-driven economies without adequate and/or nascent regulation, the Asian region poses special challenges to data protection. In fact, divergence in regulatory regimes, translating into different principles and legal basis of data protection (unlike a uniform guide like the GDPR in Europe),[63] the specific impact of a portability right might vary across nations (discussed in the following sections). However, some common issues that might arise taking the developing Asian countries as the paradigm are detailed here.

One, the overall issue highlighted in Section II regarding the lack of awareness about the right is heightened in a developing country where digital literacy is deficient as is. Even if the masses know about the existence of the right, the means to exercise it may not be accessible, either for the low digital penetration, or for lesser proficiency in technology.[64] The huge digital divide between rural and urban areas as well as people of different genders and income levels[65] may render the right to data portability 'a right of the privileged'. The issue is all the more critical

---

es%20DUOMENU%20SUBJEKTAMS%202019-10-16.pdf; French Data Protection Authority: https://www.cnil.fr/fr/le-droit-la-portabilite-obtenir-et-reutiliser-une-copie-de-vos-donnees.

[62] *Uber drivers v. Uber,* DISTRICT COURT OF AMSTERDAM, NETHERLANDS, ECLI:NL:RBAMS:2021:1020 (11 March 2021), para 4.80, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1020; *Ola drivers v. Ola Cabs*, DISTRICT COURT OF AMSTERDAM, NETHERLANDS, ECLI:NL:RBAMS:2021:1019 (11 March 2021), para 4.59, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1019.

[63] *Data Privacy Challenges For The Asia-Pacific Region*, RISK & COMPLIANCE MAGAZINE, https://riskandcompliancemagazine.com/data-privacy-challenges-for-the-asia-pacific-region.

[64] *South Asia's Digital Opportunity: Accelerating Growth, Transforming Lives*, WORLD BANK (2022), http://hdl.handle.net/10986/37230.

[65] Yoonee Jeong, *Bridging the Digital Divide*, EAST ASIA FORUM (7 July 2022), https://www.eastasiaforum.org/2022/07/07/bridging-the-digital-divide/.

because it is the digitally illiterate whose personal data is more vulnerable to collection and processing in the first place without their knowledge.

Two, stemming from the point above, consent is often illusory or artificial for people who are incapable of comprehending the implications of their data being processed. Terms and conditions couched in a long and complicated form as well as vague prescriptions on what constitutes consent disproportionately affects such population. For instance, the ASEAN framework on data protection does not adequately define the nature of consent, in addition to being a mere guiding document. Similarly, APEC's Privacy Principles are criticized as being inconsistent.[66] A country-specific example is Singapore, which amended its Data Protection Act in 2020, to provide several exceptions to the requirement for seeking consent.[67]

Three, there is a lack of digital accountability and transparency standards in the Asian countries, especially related to the functioning of artificial intelligence, despite the values being adopted as principles by transnational organizations such as OECD[68] and APEC[69]. However, these organizations only provide policy prescriptions and thus are not binding on individual countries. As a result, nations like Japan[70] and India[71] have not explicitly mandated data controllers to follow requirements of accountability and transparency like the GDPR in their respectively existing data protectional frameworks. Such a deficiency directly impacts the ability of data principals to control their data including verification of the amount of data collected and stored with the controller. Thus, a meaningful exercise of the portability right is not ensured.

Four, a major concern with the implementation of the right in general is the cost to be borne by the data controller in complying with a portability request, which includes developing systems that enable portability, collection and verification of requests, and execution of the portability. So, small players operating in the market would be more susceptible to be found in breach of the right. While solutions range from charging the principal for making a request to

---

[66] Leon Trakman, Robert Walters & Bruno Zeller, *Digital Consent And Data Protection Law – Europe And Asia-Pacific Experience*, UNSWLRS 10 (2020), p. 8.

[67] Personal Data Protection (Amendment) Act, 2020, No. 40 of 2020 (Singapore), Clause 6(6).

[68] O.E.C.D., *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (Adopted 22/05/2019).

[69] A.P.E.C. Privacy Framework (2015).

[70] Act on the Protection of Personal Information, Act No. 57 of 2003 (Japan).

[71] Digital Personal Data Protection Act, 2023, No, 22 of 2023 (India).

differential application of the right,[72] a determination as to the exact application of any chosen solution is onerous in a developing country looking for digital penetration towards masses that are incapable of affording to spare money for porting their data and/or are unaware of the extent of their rights.

Though most of these concerns are common across data protection principles, discussing them in a portability context nevertheless remains important so as to consider the specific right while developing solutions to respond to the general challenges. Further, it is observed that a majority of these issues arise in implementation of the right which should be taken into account to affect the phraseology of the right itself.

While this details the general complications associated with the RtDP in Asia, we must test the viability of the right specific Asian countries including the narratives present in India, taking into account all of the problems and achievements of the right in various jurisdictions.

(i) China

Article 45 of the PIPL has the right to data portability. As per this right, an individual can "consult and copy their personal information from personal information handlers." The obligation of the handlers are to do it in a timely manner and in case of request to transfer it to some other handler, to provide a channel for the same. There are a couple of exceptions to this right as well - first, where the laws deem it to be confidential, and second, where the state's organs' fulfilment of their statutory duties and responsibilities requires precedence.[73]

While this describes the current model of portability in China, the idea of the right to data portability has had a sectoral existence even before the formulation of the PIPL and was present either in discussions or in laws for consumer protection, telecommunication, e-commerce, etc.[74] Further, these references have also been in case laws, from which the interpretation of the right in China would draw from.

[72] Priyanshi, *Data Portability under India's Personal Data Protection Bill and Competition law in the digital sector: Key takeaways from the GDPR*, KLUWER COMPETITION LAW BLOG (12 Feb. 2022), https://competitionlawblog.kluwercompetitionlaw.com/2022/02/12/data-portability-under-indias-personal-data-protection-bill-and-competition-law-in-the-digital-sector-key-takeaways-from-the-gdpr/.

[73] Privacy and Information Protection Law (PIPL), art. 45.

[74] Meiling Xu, "*Data Portability" in China: The Controversy, the Status Quo, and Future Prospects*, PYMNTS (January 29, 2021), https://www.pymnts.com/cpi_posts/data-portability-in-china-the-controversy-the-status-quo-and-future-prospects/.

For instance, there has also been long discussion over the idea of data being an "intangible asset" and hence, the user's property.[75] While the main idea behind data portability generally has been the prevention of user lock-in, this discussion implies that the portability aspect can be a result of claim over data as a property right by the user. However, this might raise questions on the distinction of data as between data provided by the user, and the observed data. While it is reasonable that the former would be a data principle's property, the latter would invite contestations between the user and the intermediary.

This interpretation would be further exacerbated by the fact that the right is not limited to the data provided by the user.[76] Thus, whether the observed data would make up a part of the data portability option is a grey area in the Chinese legislation as well.

Furthermore, it is noteworthy that the PIPL doesn't provide for any requirement for the data to be in a specific given format of machine readable, structured etc. This could be a potential regard for not having the data portability right properly enforced and implemented.

(ii) Philippines

The Data Privacy Act 2012 of the Philippines states that in cases where personal information is being electronically processed and in a format that's organized and widely utilized, individuals have the right to request a copy of the data being processed from the controller of said personal information. The copy should be provided in an electronic or organized format, commonly accepted, and should enable the individual to further utilize the data as they see fit. As such, the right is quite similar to GDPR RtDP.

One additional factor present in the Philippines is mandating of "technical standards, modalities and procedures for their transfer". This is a requirement which has an effect on the actual implementation of the act, and takes into account the gaps left behind in the GDPR.

(iii) Japan

While Japan doesn't currently have a right to data portability, the discussions on the same have been underway for a long time, with there being working groups that study the right as well. One such study was undertaken by the Study Group on Competition Policy for Data Markets organized under the Competition Policy Research Centre of the Japan Fair Trade Commission,

[75] (2017) Zhejiang 8601 Minchu No. 4034; (2018) Zhejiang 01 Minzhong No. 7312.

[76] Anja Geller, *How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective*, 69 GRUR INT'L 1191 (December 2020), https://doi.org/10.1093/grurint/ikaa136.

which gave forth a policy understanding of the same, and captured the discourse of Japan on the right.[77] As per these studies, the GDPR system of a right to data portability lacks on many accounts and a proper policy on the same would require many changes.

Firstly, the suggestion included the classification of the platforms to be more layered than just the size (analogical to platforms in the intermediary liability rules of India), but also require considerations such as differential data (industrial, personal or non-personal like in the GDPR), and the sector in question (level of maturity). Secondly, the position of the stakeholders in this question needs to be clear. A right to data portability can be user centric, platform centric, or somewhere in the middle in its approach, but in that, the effectiveness of the data portability must be kept into consideration. Thirdly, the aspect of regulated self regulation is proposed whereby the rules guiding the operations of portability and interoperability would be set up by the intermediaries themselves. There would be a need to have a body that can affirm certain actions or question others in this context or necessary governmental intervention to set minimum thresholds, so as to address the possibility of self dealing.[78] Lastly, since the right has interconnection and relation to so many other sectors, all of them need to be looked at in a balanced manner and with a full sectoral view into things.

(iv) Other Asian Jurisdictions

Apart from these, the discourse in a few other Asian regions also persists. In Singapore, the 2020 Amendments brought about in the Personal Data Protection Act led to the inclusion of the right to data portability, however, it still remains to be enforced.[79] In Thailand's legislation, there is complete mirroring of the provisions of the GDPR. In South Korea, while initially the data protection law did not have the right to data portability, the new amendments to it have brought about a major overhaul in terms of the user rights. This includes the introduction of the right to data portability.

(v) Right to Data Portability in India

[77] Report of the Study Group on Competition Policy for Data Markets, https://www.jftc.go.jp/en/cprc/reports/studygroups/index_files/210817_report_en.pdf

[78] Parkinson, J. E., '*Management Self-Dealing', in Corporate Power and Responsibility: Issues in the Theory of Company Law, Clarendon Paperbacks,* OXFORD, 1995; ONLINE EDN, OXFORD ACADEMIC, (2012) https://doi.org/10.1093/acprof:oso/9780198259893.003.0023 (last visited 31 Aug. 2023).

[79] Personal Data Protection Commission, Discussion paper on Data Portability (2019) https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf

The data economy in India is rapidly growing, with programmes like 'Digital India' boosting the digitization move. People are increasingly availing digital services, and more and more data is being generated every second.[80] This necessitates the enactment of a comprehensive data protection framework, which ideally must include granting data subjects the right to data portability. However, the recently passed Digital Personal Data Protection Act of 2023 lacks any mention of the right. This is especially alarming since the previous version of the bill, the Personal Data Protection Bill, 2019 ("**PDP Bill, 2019**") did contain such a provision.

While the utility of the right is still questionable, a complete omission of the right is undesirable considering its inherent advantages (as discussed under Section I). Still, this part attempts to understand the right, as used in the PDP Bill, 2019 to gain insights into the Indian parliament's approach to the right as compared to the EU GDPR.

Clause 19 of the PDP Bill, 2019, which contains the right is evidently based on Article 20 of the GDPR, allowing both direct and indirect portability. Further, the scope of the right is limited to processing done by automated means, as in the GDPR. Upon exercise of the right, the data may be provided to the data principal in a 'structured, commonly used and machine-readable format'. However, the bill failed to define the three terms, leading to possible semantic difficulties had the right been implemented.

Still, there are notable differences and departures from the GDPR, the most prominent one being that the right can be exercised even for generated and inferred data (see Clauses 19(1)(a), sub-clauses (i) and (ii)). Two, there is no requirement for the processing to be carried out consensually or under a contract as in the GDPR. These factors make the portability right under the PDP Bill broader than the GDPR.

On the other hand, the right envisaged under the PDP Bill is narrower as it makes exceptions to the right on grounds of functions of state and revelation of trade secrets. Both the exceptions are worded very broadly, potentially making huge carveouts from the right, essentially defeating its purpose. The former could be extended to immune the state from being obligated to port data entirely,[81] the latter is a dynamic concept and thus cannot be a ground to deny the

[80] *Digitalizing India: A Force to Reckon With*, EY INDIA (7 Feb. 2023), https://www.ey.com/en_in/india-at-100/digitalizing-india-a-force-to-reckon-with.

[81] *India's Data Protection Bill: Further Work Needed In Order To Ensure True Privacy For The Next Billion Users*, ACCESS NOW (24 Feb. 2019), https://www.accessnow.org/wp-content/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf.

right, as opined by the Joint Parliamentary Committee constituted to analyse the bill.[82] In fact, the conflict between disclosure of trade secrets and rights of data subjects has been discussed in the European Parliament, and it was opinionated that rights should prevail over protection of trade secrets.[83]

Secondly, the text of the right does not provide protection to rights and freedoms of others against an exercise of the portability right. Hence, unlike the GDPR, Clause 19 of the PDP Bill disregards the privacy of third-parties altogether, occasioning disclosure of their personal data to unauthorized persons upon an exercise of portability by another person.

Thirdly, the data fiduciary can refuse furnishing data directly to user if it is not technically feasible, which GDPR provides the defence only for cross transmission between controllers. This further restricts the scope of the right. Even the BN Srikrishna Committee Report suggests the defence only for data transfers to other fiduciaries.[84]

Thus, while clause 19 borrows heavily from Article 20 GDPR, the right granted therein is both wider and narrower in respect of different aspects, indicating differential impact had the provision been enacted. But considering that it was not so done, an in-depth analysis of such impacts is not feasible.

3. Right to data portability in India – a proposition

Thus, deriving from the above-mentioned analysis of the right in isolation, in the GDPR, in other Asian jurisdictions, and the discourse around it in India, there needs to be a comprehensive right that needs to be envisaged, instead of a legislation which might not find a lot of practical implementations. This section thereby attempts to enlist a set of points that would be crucial to either formulate this right freshly, or adapt the GDPR one to India.

---

[82] *Report of the Joint Committee on The Personal Data Protection Bill, 2019*, SEVENTEENTH LOK SABHA (Dec 2021), p. 78, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

[83] *Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure* (12 Mar. 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf.

[84] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, p. 75, https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf.

One, the definitions of the terms employed to describe the right have to be detailed and must define the nuances for the same. The data that can be ported has to be defined well. The GDPR definition of data that is provided by the user has to be enlarged to fit both the collected data and the generated data,[85] as discussed previously. Further, the grounds for "structures, commonly used, and machine readable" must be listed down in full details. This would help curb the negligent implementation of the right that has been prevalent.[86] However, a detailed definition should also not imply that the right in itself might be blocked if a provision isn't complied to. For instance, instead of being like the GDPR which only broadly tells that that the third part rights must not be violated, or like the PDP which completely disregards this aspect, there should be a provision detailing that the rights of the third party should not be violated, and where violated, only the data that violates these rights cannot be ported, and the right in itself will not be blocked as a whole.

Two, the fact that the DPDP Act excludes the data that is processed for personal purposes or made publicly available might have an effect of not including a majority of the content that would generally be ported, if defined in the distinction of personal or non personal data.[87] Thus, an alternative way to go about it should be on the ascribing of value to data instead of the aforementioned distinction, where the data controller charges for the services that they provide even non-personal information should be subject to the RtDP since there the cost of the service is actual money paid by the data principal .[88]

Three, along with the standard format the technology and system developed by the significant data controllers must be mandatory shared with the industry as a whole so that the concerns of interoperability and the liability of the smaller data controllers to develop such systems are overcome. Thus, in a situation where the smaller data controllers have to port the data to the user, they can do so under minimum switching costs, and in a situation where they have to port the data to the significant data controllers, they may charge the significant data controllers for

---

[85] Right to Data Portability, ICO (last visited [August 31, 2023]) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/#:~:text=Sometimes%20the%20personal%20data%20an,using%20a%20device%20or%20service

[86] Kuebler-Wachendorff, S., Luzsa, R., Kranz, J. et al., *The Right to Data Portability: Conception, Status Quo, and Future Directions,* 44 INFORMATIK SPEKTRUM 264, 272 (2021), https://doi.org/10.1007/s00287-021-01372-w.

[87] Sec. 3(c) of the Digital Personal Data Protection Act, 2023.

[88] Zufall, F., & Zingg, R., *Data Portability in a Data-Driven World, in Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* 215-234, CAMBRIDGE UNIVERSITY PRESS (2021), doi:10.1017/9781108954006.012.

this. In turn, to make this system efficient, instead of classification of the data controllers on the basis of the number of users, factors such as revenue turnover,[89] or the number of competitors they have should be used to define the system's size. Thus, there has to be a differential treatment of the platforms for data portability to be efficient.[90]

Four, delegated legislation or the self regulatory guidelines should provide for the manner in which a data portability request should be processed, including a designated officer, such as a compliance offer, to whom the request should be addressed. Further, a timeline for the complete processing of the same has to be given for it to be actually implemented.[91] However, to eliminate a situation where the option of data portability and interoperability may allow for attacks, when it comes to sectors more prone to data security breaches, such as hospitals or scientific research areas, the presence of expert designed high level industry compliances is a must. This differential application would allow for smoother portability with lesser threats of events such as the Cambridge Analytica analogy of an open API.[92]

Five, the problem of consent and general understanding of the right can only be tackled by mass awareness of the scheme, something that is majorly lacking in a nation like India. Thus, with the development of the provision for the right to data portability and even the general data protection regime, there have to be steps taken by the state to educate the people on their rights. Without this, the ground level implementation of a right like this cannot happen.

Lastly, apart from the legislative points to be kept in mind, the technological developments have to also be taken into account. Thus, deeper research and understanding has to go into the technologies of edge computing and APIs for the transition to a regime with the right to data portability to be smoother.[93]

Conclusion

[89] Sonja Solomun, Maryna Polataiko & Helen A. Hayes, Note, *Platform Responsibility and Regulation in Canada: Considerations on Transparency, Legislative Clarity, and Design,* HARV. J.L. & TECH. DIG. (2021), https://jolt.law.harvard.edu/digest/platform-responsibility-and-regulation-in-canada-considerations-on-transparency-legislative-clarity-and-design.

[90] Bart van der Sloot Engels, *Data Portability Among Online Platforms*, 5 INTERNET POL. REV. 2 (2016), https://doi.org/10.14763/2016.2.408.

[91] Michael A Cusumano et al., *Can Self-Regulation Save Digital Platforms?,* 30 INDUS. & CORP. CHANGE 1259, 1285 (October 2021), https://doi.org/10.1093/icc/dtab052.

[92] Improving Consumer Welfare with Data Portability, by Daniel Castro (November 29, 2021), Centre for Data Innovation, https://www2.datainnovation.org/2021-data-portability.pdf.

[93] Wong, J., & Henderson, T., *The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR*, INTERNATIONAL DATA PRIVACY LAW, https://doi.org/10.1093/idpl/ipz008.

The paper discusses the right to data portability in a holistic manner, discussing the criticisms levelled against the right and the challenges it poses. While we begin with a global perspective, taking the GDPR as the guiding document, our point of focus is the status of the right in Asia and the specific issues that arise with the Asian ideas of the portability right. We find that unlike Europe, there exist wide divergences between how the right is perceived in various Asian economies, even though the respective provisions are evidently based on Article 20 of the GDPR. While some countries have recognized and made adjustments to meet the shortcomings associated with GDPR, others have enacted even more vague provisions. However, like in Europe, portability is still largely an under-utilized and paper right.

Hence, through our recommendations, made strictly from a data protection point of view, we have attempted to provide a means to address the concerns identified throughout the paper. By no means are the recommendations fool-proof, but they may be considered a starting point for drafters and executors of a portability right. The foundation is to make the right unambiguous enough so that it is implementable and to implement it in its spirit.