Informatik Spektrum (2021) 44:264–272
https://doi.org/10.1007/s00287-021-01372-w

HAUPTBEITRAG

The Right to Data Portability: conception, status quo, and future directions

Sophie Kuebler-Wachendorff[1] · Robert Luzsa[2] · Johann Kranz[1] · Stefan Mager[1] · Emmanuel Syrmoudis[3] · Susanne Mayr[2] · Jens Grossklags[3]

Accepted: 1 June 2021 / Published online: 6 July 2021

Abstract

For almost three years, the General Data Protection Regulation (GDPR) has been granting citizens of the European Union the right to obtain personal data from companies and to transfer these data to another company. The so-called Right to Data Portability (RtDP) promises to significantly reduce switching costs for consumers in digital service markets, provided that its potential is effectively translated into reality. Thus, of all the consumer rights in the GDPR, the RtDP has the potential to be the one with the most significant implications for digital markets and privacy. However, our research shows that the RtDP is barely known among consumers and can currently only be implemented in a fragmented manner—especially with regard to the direct transfer of data between online service providers. We discuss several ways to improve the implementation of this right in the present article.

Introduction

Based on their market-dominating positions in core online service markets, companies such as Google, Facebook, Microsoft and Amazon are able to amass ever vaster amounts of data[1] that their users provide wittingly or unwittingly [31, 39]. These data are kept in proprietary data silos, which give firms owning these silos a competitive edge in increasingly data-driven innovations, especially in artificial intelligence. In fact, Google's former director of research, Peter Norvig, stated that the company "does not have better algorithms, [but] just more data" [30]. Thus, for competitors or new market entrants, these large proprietary data silos owned by dominant digital platform providers have erected high barriers for innovation and have led to a skewed level playing field [17, 20, 33]. On the other hand, these dominant market players have leveraged their data to expand in numerous other online and offline markets.

A digital platform is an "extensible codebase of a software-based system that provides core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate" [42]. Dominant online service providers (OSPs) operate digital platforms offer-

Sophie Kuebler-Wachendorff
kuebler-wachendorff@bwl.lmu.de

Robert Luzsa
Robert.Luzsa@uni-passau.de

✉ Johann Kranz
kranz@lmu.de

Stefan Mager
stefan.mager@lmu.de

Emmanuel Syrmoudis
emmanuel.syrmoudis@tum.de

Susanne Mayr
Susanne.Mayr@uni-passau.de

Jens Grossklags
jens.grossklags@in.tum.de

1 Internet Business and Internet Services, Ludwig-Maximilians-Universität München, Ludwigstraße 28, 80539 München, Germany

2 Psychology and Human-Machine Interaction, Universität Passau, Dr.-Hans-Kapfinger-Str. 14b, 94032 Passau, Germany

3 Cyber Trust, Technische Universität München, Boltzmannstraße 3, 85748 Garching, Germany

[1] The BBC estimates that those four companies alone own at least 1200 petabytes or 1.2 million terabytes of data, see https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/.

ing a large variety of online services such as search, social networking, commerce, messaging, mail, smart assistants, streaming and payment that have become essential to the lives of billions of users [11]. Owing to positive network effects, users are locked-in to the services of these dominant OSPs [11, 37]. Since the services are essential for users, accompanied by substantial lock-in effects and switching costs, dominant OSPs are virtually incontestable [15]. As a result, not even several high-profile data scandals (e.g. Facebook's Cambridge Analytica case or Equifax's data breach) and the growing public awareness of data misuse have led to a considerable number of users switching to alternative services [22, 47].

As a consequence, these platforms grow ever more powerful in their primary markets and leverage their data silos, market power and installed user base to enter other markets. For instance, beyond internet search, Google's parent company Alphabet is active in over 14 ventures as diverse as autonomous driving (Waymo), smart home appliances (Nest) and payment (Google Pay), which leverage Alphabet's proprietary data silos in various ways. For a number of reasons, European companies lack those rich data sets, which endangers future competitiveness and innovativeness not only in online markets, but also in digitally transforming physical industries [20]. Therefore, an increasing number of policy makers, firms and consumer advocates call for action to revitalise competition and to level the playing field in the digital economy [13, 14, 17, 26, 33, 36, 43].

To strengthen users' data sovereignty and enable data interoperability between online services, the General Data Protection Regulation (GDPR) has introduced data portability as a new fundamental right to users.

Article 20 of the GDPR specifies the Right to Data Portability (RtDP) as follows:

> 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
> (a) the processing is based on consent pursuant to point (a) of Article 6 (1) or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and
> (b) the processing is carried out by automated means.
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The RtDP comprises two sub-rights. First, the right to export data, which allows individuals to request and receive their personal data in a structured, commonly used and machine-readable format. Second, the right to directly transfer data, which allows individuals to request a direct data porting from one OSP to another. Hence, the RtDP is aimed at decreasing switching costs and lock-in effects and facilitate competition in highly concentrated digital service markets [7, 25]. Beyond increasing users' privacy, the RtDP could further serve as the gateway for individuals to participate in the data economy and profit from the immaterial wealth of their personal data [7]. However, while the RtDP is a powerful user right that could strengthen users' choice and privacy and spur competition in "tipped" digital service markets, how the RtDP should be implemented in practice has been left open by legislators [7].

First, the scope of personal data "which he or she has provided to a controller" (Art. 20 (1) GDPR) is unclear. In principle, the scope of data can be distinguished into four possible dimensions [7, 27]. Received data refers to direct inputs by users, such as a restaurant review. Observed data refers to data collected by sensors, such as restaurant location data collected by GPS. Inferred data encompasses data created by the OSP based on received and observed data, such as favourite cuisine and restaurant. Predicted data only indirectly analyses actual reality and anticipates future prospects, such as the probabilistic supposition that a young adult's favourite cuisine will become more refined and expensive in the long-term. Accordingly, "provided" personal data as specified in the RtDP can either be interpreted as received data only, or as received and observed data [7]. In a more restrictive approach, the term "provided" would imply an intentional action by the user, hence only data supplied directly by the individual can be considered. The extensive approach, on the other hand, targets the overall objective of the RtDP—increasing individual data controllership—and thus employs a broader interpretation of the provision that includes data collected about users' behaviour.

Second, clear specification about the required "structured, commonly used and machine-readable" data format is lacking. The European Union (EU) has only defined the term "machine-readable" more precisely as a structured format that allows applications to easily identify, recognise and extract specific data, such as individual statements of fact and their internal structure.[2] Further, these specifications are more a required minimum, since the overarching objective is to facilitate data interoperability [2]. At present, only

[2] 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] OJ L175/1, rec 21.

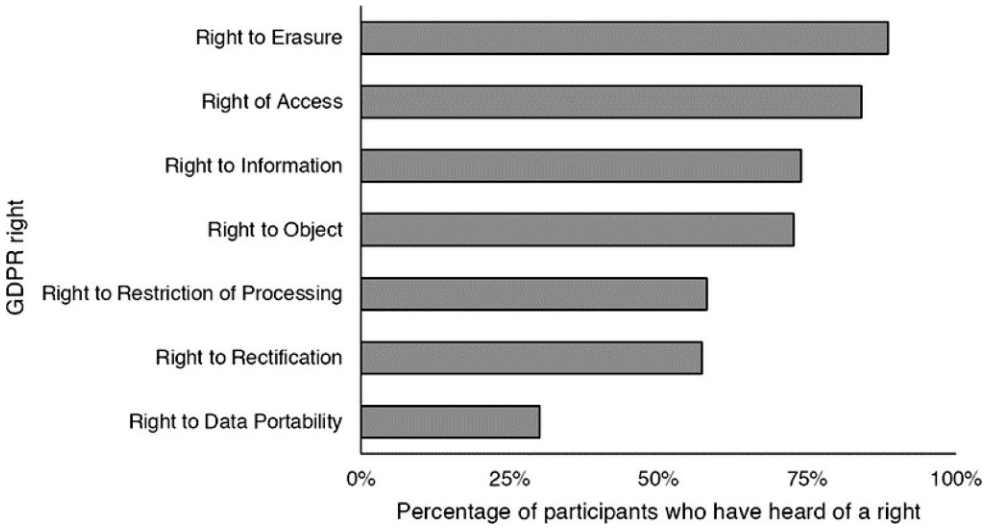

Fig. 1 Knowledge of General Data Protection Regulation rights ($N = 246$)

eight data formats (e.g. CSV, JSON, XML)[3] are deemed fully compliant with the GDPR's requirements [46].

Third, it is unclear how a direct transfer between services should work from a technical perspective. Technical obstacles include lack of standardization, compatibility and interoperability, thereby complicating data transfer between different providers of online services. Furthermore, it is crucial that users' transfer requests are easy and reliable, thus avoiding "dark patterns", i.e. user interface design choices that lure individuals into taking unintended and potentially harmful options [4, 29]. The RtDP also creates several technical privacy and security challenges such as interdependent privacy considerations that address data associated with multiple individuals, e.g. social connections [34, 35, 44]. Further, the RtDP, like the Right to Access, harbours considerable security vulnerability, as a lack of standards and poor request practices create room for impersonation by merely bypassing one authentication step, and thus gaining access to extensive and sensitive user data [8, 18].

In the following sections, we report on three studies that we conducted to analyse the current state of individuals' awareness of the RtDP, their motivations to switch between OSPs (section on *Users' knowledge and motivation*) and the current best practical application of the RtDP (section on *Current effectiveness of the Right to Data Portability*). The article concludes with a discussion of our findings and avenues for future research.

Users' knowledge and motivation

In order for data portability to be successful, it is crucial to understand both the current level of online users' awareness of their RtDP, as well as the potential of the RtDP to act as a facilitator for consumers to switch services. Therefore, we conducted two online surveys with German internet users (predominantly students) to explore these questions[4]. The first study focused on users' knowledge of the rights guaranteed in the GDPR ($N = 246$), while the second study examined users' motivations to switch between OSPs and the possible facilitating role of data portability for switching behaviour ($N = 227$).

Regarding knowledge of GDPR rights, the results are in line with previous surveys [12, 38]: the RtDP is the least known right of the GDPR, with less than a third of participants indicating that they have heard of it. For all other rights, more than half of the participants reported having heard of the respective right before, including the Right to Data Erasure, which was familiar to 89% of the participants (Fig. 1).

A similar pattern emerges when participants are asked how well they understand the meaning of each GDPR right (Fig. 2): participants rated data portability as the most elusive and difficult to grasp correctly, while all other rights were rated as more comprehensible, with the Right to Erasure appearing as the easiest to understand.

These results demonstrate that some GDPR rights appear to be widely known and comprehensible to users, perhaps partly due to the attention media paid to the Right to Erasure when the GDPR became effective in 2018. Regarding other rights, and especially the RtDP, there is still a consid-

[3] Compliant file formats: CSV, EML, ICS, JSON, MBOX, TEX, VCS, XML [46].

[4] For a detailed description of these studies in German, see www.bidt.digital/blog-datenportabilitaet.

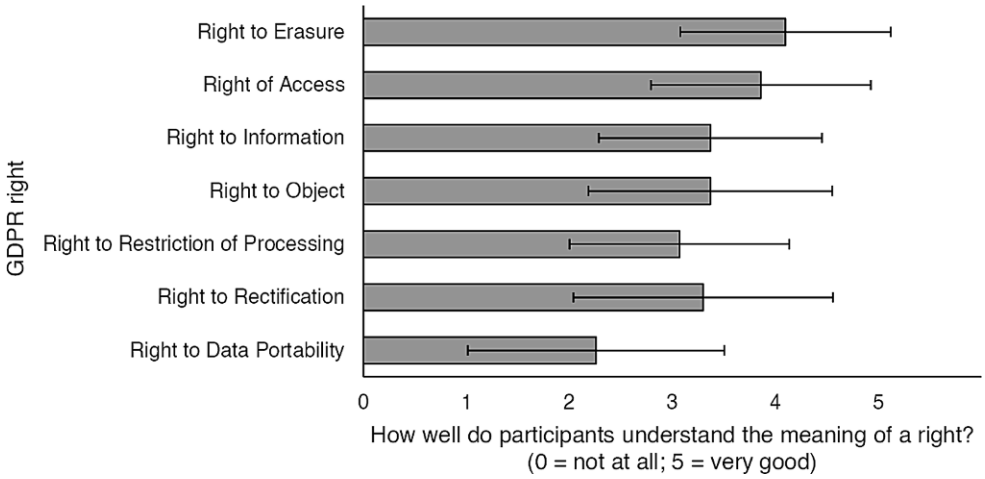

Fig. 2 Understanding of the meaning of General Data Protection Regulation rights ($N = 246$, *error bars* indicate ±1 standard deviation)

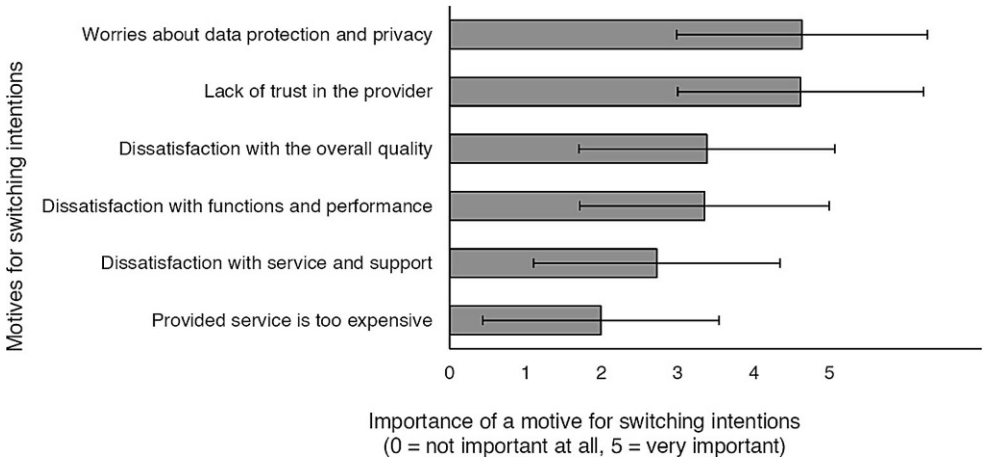

Fig. 3 Motives for online service provider switching intentions ($N = 227$, *error bars* indicate ±1 standard deviation)

erable lack of knowledge and a need for information and education.

Despite this lack of awareness, the second study on OSP switching motivations illustrates that there is a significant need for simple and user-friendly data portability solutions. Participants were asked to indicate which OSPs (e.g. social networks like Facebook, cloud storage solutions like Dropbox) they use and whether they consider leaving or switching these services. Then, based on the push–pull–mooring framework of service migration [3], users with switching intentions were asked for their motives and for perceived obstacles preventing them from switching.

Overall, participants indicate in 10.3% of all cases that they have the intention to leave their current OSPs and/or would like to switch to another service, but have not yet done so.

Regarding switching motives, users appear mostly driven by concerns about data security and privacy, as well as a general lack of trust in the current service provider, followed by dissatisfaction with quality, performance and support provided by the service. The financial aspects were rated as the least important reason to switch services (Fig. 3).

But what keeps users from switching to more secure and privacy-oriented providers? The main obstacles mentioned are a lack of knowledge about comparable, alternative providers (52.25%), a lack of experience with switching between providers (32.30%) and the fear that switching could be complex and involve loss of data and information (22.47%). Additionally, 66.4% of all participants stated that the inability to port their data from their current to another provider plays a major inhibiting role.

In summary, while the study findings cannot be fully generalised due to a lack of representative samples, their findings emphasise that the RtDP addresses real and widespread needs among online service users and that it could significantly empower them in regard to their ability to easily switch between providers. However, the results also underline the crucial role of information and the lack thereof, given that most users are not aware of their RtDP and also know little about alternatives to their current OSPs.

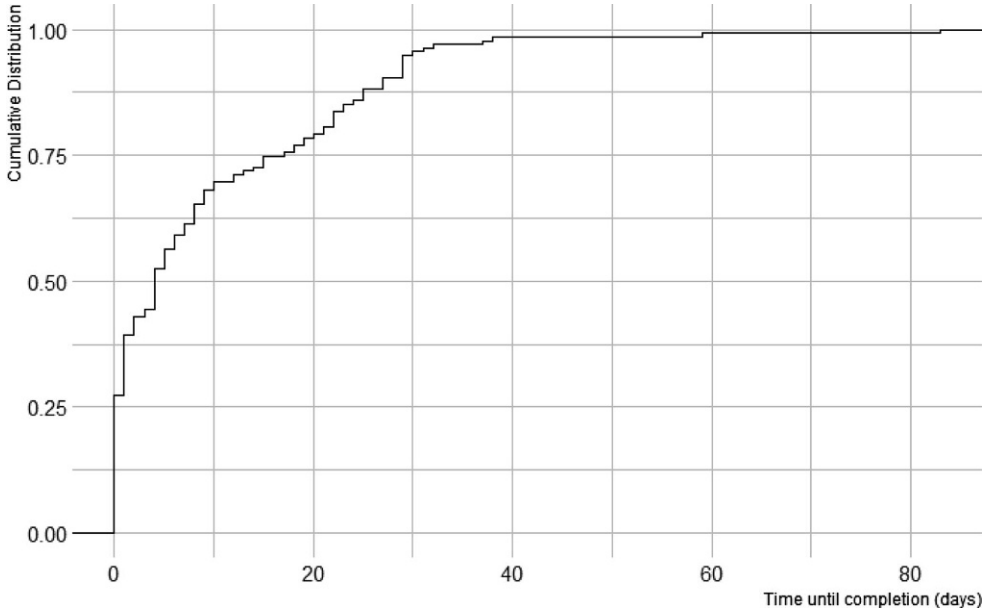

Fig. 4 Duration of data export responses: requests on the Right to Data Portability

Current effectiveness of the right to data portability

Once an individual possesses the necessary knowledge and motivation to transfer personal data between OSPs, successful execution of the RtDP depends on its practical feasibility. We therefore conducted an empirical analysis on the effectiveness of the RtDP to systematically assess the feasibility of transferring data between services based on a sample of 182 online services [41].

In the analysis, we distinguish between *direct* and *indirect data portability*. The former can be thought of as the implementation of the GDPR Art. 20 (2) GDPR aspiration: the feasibility of a direct data exchange between a majority of corporations in (a certain industry of) the economy. However, individuals cannot make use of *direct data portability*, as the necessary infrastructure is still missing. While some projects, such as the Data Transfer Project and the Data Portability Cooperation, are under development, building such an extensive infrastructure is a complex and timely endeavour that is far from being complete. Hence, users aiming to transfer their data to a new OSP have to make use of *indirect data portability* (GDPR Art. 20 (1)). This implies that users have to request a copy of their personal data from the current provider and request a new provider to import the data or import the data manually. As solutions enabling *direct data portability* are virtually non-existent, we could only analyse *indirect data portability*.

We first assessed the data export requests in terms of duration and adherence to the legal timeframe, followed by compliance with the file format, and the data scope provided, and lastly we analysed the import requests based on the options provided. Our overall results show a vast discrepancy between the intention of GDPR Art. 20 and the current implementation of the law. First, in terms of exporting personal data, 74.2% or 135 of the 182 OSPs provided data exports within the legally permitted timeframe (see Fig. 4). Only these 135 service providers were considered for further analysis, of which merely 51.1% (69 providers) were able to meet the requirement of a "structured, commonly used and machine-readable" data format and provided exported data that could be imported with relatively little effort at another service provider [41]. Fig. 5 shows our results.

Further, we analysed the scope of exported data [7]. All 135 OSPs exported at least parts of received data, 96 providers additionally delivered observed data, of which 12 OSPs even exported some inferred data (see Fig. 6). Taking the restrictive approach, i.e. "provided" data (GDPR Art. 20 (1)) includes only received data, a total of 101 service providers exported all personal data actively provided [41].

Concluding on the duration, format and data scope assessment, of the 182 OSPs in our sample, only 52 service providers (28.6%) have fulfilled all requirements and are therefore compliant with GDPR Art. 20 (1). Consequently, 130 OSPs (71.4%) failed regarding at least one requirement.

The second step of *indirect data portability* requires users to import data at the new service. Therefore, as a final step, we analysed data import options that the services in our sample offered. Contrary to the intentions of policy makers that the RtDP would encourage firms to make imports as easy as possible, we found that the majority of services in our sample (76.8%) did not offer any data import options at all (see Fig. 6). Only 44 services (23.2%) provide users at least some data import features.

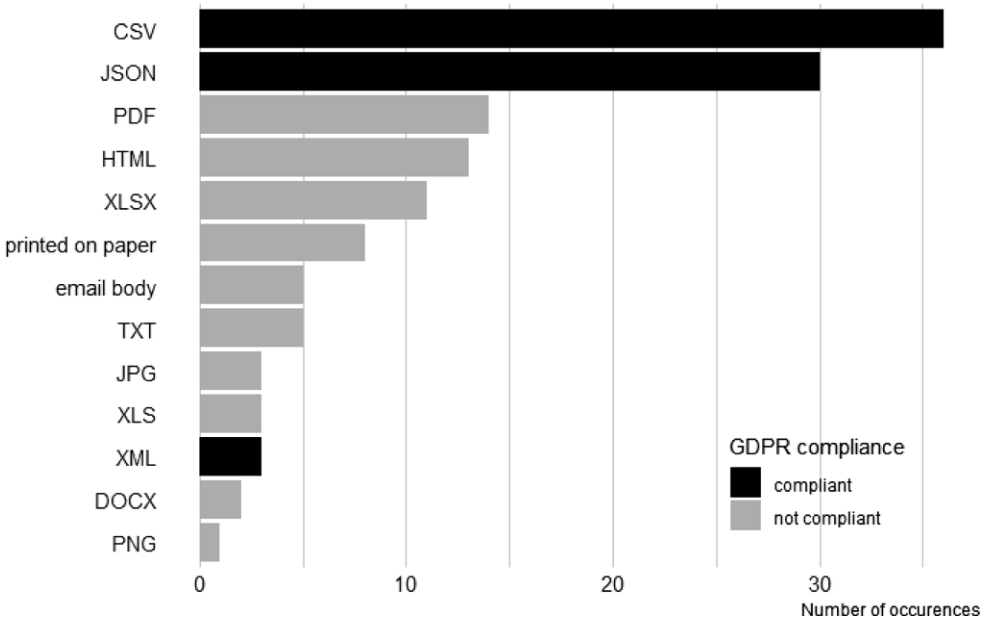

Fig. 5 Format compliance with the Right to Data Portability

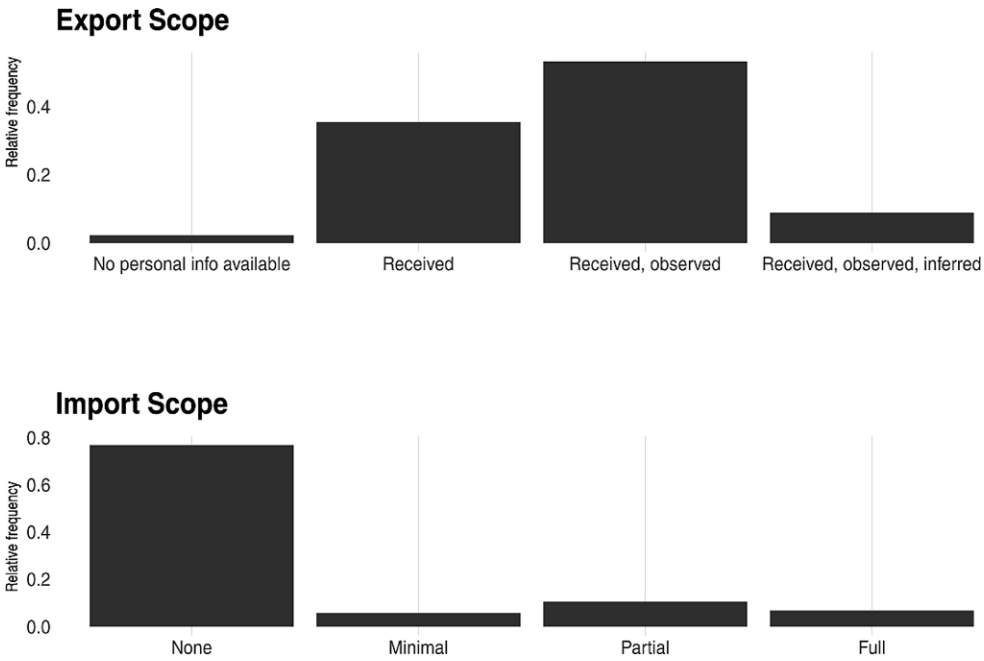

Fig. 6 Data export scope and import options provided by the online service providers

While 31 OSPs offered only minimal or partial data import options, 13 service providers facilitate full data upload [41].

Discussion and future steps

Our results show that the RtDP is currently a blunt sword that does not live up to its potential to spur competition in highly concentrated digital markets and increase users' privacy and control over data. Less than one in four OSPs offered users the possibility to import data from other online services. Looking at these results, it becomes evident that OSPs and regulators must make significant progress to implement the RtDP in such a way that it could deliver on its promises in the future. Three years after the GDPR became effective in the EU, the RtDP is more a regulator's brainchild that users are barely aware of and use. Also, rivals of dominant OSPs do not leverage the RtDP to attract users with features that allow them to easily switch to their services. We identified a lack of awareness and motivation amongst users and a lack of easy-to-use data portability

tools, techniques and practices for data export and import as core problems. In the following, we discuss possible ways to address both shortcomings in order to increase the effectiveness of data portability.

Regarding users' lack of knowledge of data portability and privacy-friendly alternatives to the currently dominating online services, studies are necessary that develop sound approaches to increase both users' awareness as well as their self-efficacy, that is, their belief of being able to successfully transfer their data when switching OSPs. For this, public information campaigns that inform about the RtDP, how to actually exert it and how to judge providers in regard to data privacy and security could be designed and evaluated. Psychological models of behaviour change, such as the Rubicon Model [1, 16, 21] and the Transtheoretical Model of Behavior Change [9, 32], may serve as a theoretical basis, for example by identifying different stages of OSP switching and by providing approaches on how to best support users in each of these via informational or motivational interventions.

Future analyses on individuals' motivation and intention to make use of the RtDP could also consider theoretical concepts, such as the privacy calculus—analysing the effects of personal beliefs on intention, privacy paradox—explaining the gap between privacy concerns and actual behaviour, or even privacy fatigue—reflecting individuals' weariness towards privacy issues [6, 10, 19]. Some of these concepts are particularly interesting when investigating the virtually non-existent reaction to data scandals, such as Cambridge Analytica. While the Federal Trade Commission fined Facebook $5 billion in 2019 in response to the data exploitation of 87 million Facebook users, it was criticised shortly thereafter for failing to introduce adequate privacy and security measures [23]. Nevertheless, Facebook has not suffered any major long-term setbacks in terms of either the number of users or the stock market.

Regarding the lack of practicably usable data portability tools, future studies may examine how offering data import or export possibilities impacts users' perceptions of an OSP. For this, users could be experimentally confronted with variations of OSP descriptions that either mention or do not mention the option to import or export data. Thereafter, OSPs might be rated by the users with regard to their perceived credibility and trustworthiness, as well as the willingness to use the service. If positive effects of data portability options can be observed (i.e. OSPs that offer data import or export options are perceived as more trustworthy and are preferably selected), this could be a compelling argument for providers to offer data portability options to their users.

Reconsidering the discussion regarding "provided" personal data in the RtDP, our results on the scope of exported data show that OSPs across all industries have exported at least some of users' observed data, for instance data collected via sensors. If regulators were to demand the extensive approach including received and observed data, the RtDP could be a driving force in strengthening user's data control rights and reducing switching costs to a bare minimum [7]. For example, when switching to another navigation application, users could not only export personal data such as their home address or prior searches, but also export observed data gathered from GPS sensors. The increased data scope would decrease barriers to switching to another navigation application. Based on the imported data, the application would be able to immediately customise its service, e.g. through recommendations based on previously visited places. However, future work is needed to evaluate the usability and feasibility to reuse data for different services. For instance, when transferring data from the navigation application to a food delivery provider, data about visited restaurants could be useful, whereas data about shops visited would probably be less useful in this regard. Also, measures need to be taken into account for the sensitivity of data, e.g. for transferring interdependent data that would also compromise privacy of others.

Apart from progress in understanding which data are worth porting, the question remains as to how direct data portability is best implemented in practice. The study by Syrmoudis et al. [41] showed that less popular platforms seem to regard data portability regulation more as a burden than an opportunity for user growth. This view could be counteracted by improved education on the right's potential. Moreover, either incentives or more specific regulation could motivate corporate actors to build interfaces for data portability platforms such as the Data Transfer Project [45]. It is up to future research to investigate which method is the most promising to solve the chicken-and-egg problem of data portability platforms [5]. From a technological perspective, the data transfer process needs standardisation regarding the design of interfaces and procedures. A promising option in this regard is to decouple data storage from service provision altogether. Users could decide on which personal online data storage systems they want to manage their data and who can access what kind of data. Such individual data controllership solutions would invert the logic of data transfer in a user-friendly way, reduce lock-in effects and could promote data-driven innovation [24, 28, 40].

Acknowledgements We are grateful for funding support from the Bavarian Research Institute for Digital Transformation (bidt).

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Achtziger A, Gollwitzer PM (2009) Rubikonmodell der Handlungsphasen. In: v. Brandstätter V (ed) Handbuch der allgemeinen Psychologie—Motivation und Emotion. Hogrefe, Göttingen, pp 150–156
2. Article 29 Data Protection Working Party (2017) Guidelines on the right to data portability. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233. Accessed: 23.03.2021
3. Bansal HS, Taylor SF, James SY (2005) "Migrating" to new service providers: toward a unifying framework of consumers' switching behaviors. J of the Acad Mark Sci 33(1):96–115
4. Bridges F, Appel L, Grossklags J (2012) Young adults' online participation behaviors: an exploratory study of web 2.0 use for political engagement. Inf Polity 17(2):163–176
5. Caillaud B, Jullien B (2003) Chicken & Egg: Competition among Intermediation Service Providers. Rand J Econ 34(2):309–309
6. Choi H, Park J, Jung Y (2018) The role of privacy fatigue in online privacy behavior. Comput Human Behav 81:42–51
7. De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I (2018) The right to data portability in the GDPR: towards user-centric interoperability of digital services. Comput Law Secur Rev 34(2):193–203
8. Di Martino M, Robyns P, Weyts W, Quax P, Lamotte W, Andries K (2019) Personal Information Leakage by Abusing the {GDPR}'Right of Access. Paper presented at the Fifteenth Symposium on Usable Privacy and Security (SOUPS).
9. Dincelli E, Chengalur-Smith S (2017) Applying the transtheoretical model of behavior change to online self-disclosure. ICIS Proceedings in Seoul, South Korea
10. Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce—a study of Italy and the United States. Eur J Inf Syst 15(4):389–402
11. Easley RF, Guo H, Kraemer J (2018) Research commentary—from net neutrality to data neutrality: a techno-economic framework and research agenda. Inf Syst Res 29(2):253–272
12. European Commission (2019) Special Eurobarometer 487a: the general data protection regulation. European Commission. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886. Accessed: 26.03.2021
13. European Commission (2020) Regulation of the European parliament and of the council: on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148. Accessed: 26.03.2021
14. European Commission (2020) Regulation of the European parliament and of the council: on contestable and fair markets in the digital sector (Digital Markets Act). European Commission. https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf. Accessed: 26.03.2021
15. Farrell J, Klemperer P (2007) Coordination and lock-in: competition with switching costs and network effects. Handb Ind Organ 3:1967–2072
16. Gollwitzer PM (1990) Action phases and mind-sets. In: Handbook of motivation and cognition: Foundations of social behavior, vol 2, pp 53–92
17. Graef I, Prufer J (2018) Mandated data sharing is a necessity in specific sectors. Econ Stat Ber 103(4763):298–301
18. Grossklags J, Christin N, Chuang J (2008) Secure or insure? A game-theoretic analysis of information security games. Paper presented at the Proceedings of the 17th international conference on World Wide Web.
19. Hallam C, Zanella G (2017) Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput Human Behav 68:217–227
20. Haucap J (2019) Competition and competition policy in a data-driven economy. Intereconomics 54(4):201–208
21. Heckhausen H, Gollwitzer PM (1987) Thought contents and cognitive functioning in motivational versus volitional states of mind. Motiv Emot 11(2):101–120
22. Hinds J, Williams EJ, Joinson AN (2020) "It wouldn't happen to me": privacy concerns and perspectives following the Cambridge Analytica scandal. Int J Hum Comput Stud 143:102498
23. Hu M (2020) Cambridge Analytica's black box. Big Data Soc 7(2):1–6
24. Jones CI, Tonetti C (2020) Nonrivalry and the economics of data. Am Econ Rev 110(9):2819–2858
25. Krämer J, Stüdlein N (2019) Data portability, data disclosure and data-induced switching costs: some unintended consequences of the general data protection regulation. Econ Lett 181:99–103
26. Kretschmer T, Wiewiorra L, Krämer J, Oehler A, Horn M, Haucap J, Klein S, Hüllmann J (2018) Datenkapitalismus – eine ökonomische Betrachtung. Wirtschaftsdienst 98(7):459–480
27. Malgieri G (2016) Property and (Intellectual) ownership of consumers' information: a new taxonomy for personal data. Priv Ger 4:133
28. Mansour E, Sambra AV, Hawke S, Zereba M, Capadisli S, Ghanem A, Aboulnaga A, Berners-Lee T (2016) A demonstration of the solid platform for social web applications. Paper presented at the Proceedings of the 25th International Conference Companion on World Wide Web. Aboulnaga, Ashraf
29. Mathur A, Acar G, Friedman MJ, Lucherini E, Mayer J, Chetty M, Narayanan A (2019) Dark patterns at scale: findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), pp 1–32
30. McAfee A, Brynjolfsson E, Davenport TH, Patil D, Barton D (2012) Big data: the management revolution. Harv Bus Rev 90(10):60–68
31. Morey T, Forbath T, Schoop A (2015) Customer data: designing for transparency and trust. Harv Bus Rev 93(5):96–105
32. Prochaska JO, Velicer WF (1997) The transtheoretical model of health behavior change. Am J Health Promot 12(1):38–48
33. Prufer J, Schottmüller C (2017) Competing with big data
34. Pu Y, Grossklags J (2016) Towards a model on the factors influencing social app users' valuation of interdependent privacy. Proc Priv Enhanc Technol 2016(2):61–81
35. Pu Y, Grossklags J (2017) Valuating friends' privacy: Does anonymity of sharing personal data matter? Paper presented at the Thirteenth symposium on usable privacy and security (SOUPS).
36. Schweitzer H, Haucap J, Kerber W, Welker R (2018) Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen vol 297. Nomos,
37. Shapiro C, Carl S, Varian HR (1998) Information rules: a strategic guide to the network economy. Harvard Business Press,
38. Sideri M, Gritzalis S (2020) Are We Really Informed on the Rights GDPR Guarantees? Paper presented at the International Symposium on Human Aspects of Information Security and Assurance..
39. Spiekermann S, Korunovska J (2017) Towards a value theory for personal data. J Inf Technol 32(1):62–84

40. Sunyaev A, Kannengießer N, Beck R, Treiblmaier H, Lacity M, Kranz J, Fridgen G, Spankowski U, Luckow A (2021) Token economy. Bus Inf Syst Eng
41. Syrmoudis E, Mager S, Kuebler-Wachendorff S, Pizzinini P, Grossklags J, Kranz J (2021) Data portability between Online services: an empirical analysis on the effectiveness of GDPR Art. 20. Proc Priv Enhancing Technol 3:351–372
42. Tiwana A, Konsynski B, Bush AA (2010) Research commentary—platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. Inf Syst Res 21(4):675–687
43. VerbraucherkommissionBaden-Württemberg (2017i) Datensouveränität, -nutzung und Datenverwertung – Forderungen nach einem „update" der Wirtschafts- und Rechtsordnung als Chance für eine selbstbestimmte Datennutzung. https://www.verbraucherkommission.de/site/pbs-bw-new/get/docments/MLR.Verbraucherportal/Verbraucherkommission-Dokumente/Stellungnahmen/45VK_Stellungnahme_Datenverwertung-souver%C3%A4nit%C3%A4t-nutzung_01.12.2017i.pdf. Accessed: 23.03.2021
44. Weidman J, Aurite W, Grossklags J (2018) On sharing intentions, and personal and interdependent privacy considerations for genetic data: A vignette study. IEEE ACM Trans Comput Biol Bioinform 16(4):1349–1361
45. Willard B, Chavez J, Fair G, Levine K, Lange A, Dickerson J (2018) Data transfer project: from theory to practice. https://services.google.com/fh/files/blogs/data-transfer-project-google-whitepaper-v4.pdf. Accessed: July 2019
46. Wong J, Henderson T (2019) The right to data portability in practice: exploring the implications of the technologically neutral GDPR. Int Data Priv Law 9(3):173–191
47. Zou Y, Mhaidli AH, McCall A, Schaub F (2018) "I've got nothing to lose": consumers' risk perceptions and protective actions after the equifax data breach. Paper presented at the Fourteenth Symposium on Usable Privacy and Security (SOUPS).