scripted

Volume 15, Issue 1, August 2018

Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control

*Helena Ursic**

DOI: 10.2966/scrip.150118.42

Abstract

Data portability is a fluid concept that can be used in multiple contexts and can be defined in various ways. In the EU General Data Protection Regulation, it is given the legal status of a data subject right. The key objectives of the right to data portability in the GDPR are privacy, protection of personal data, and data subjects' control over their data. However, it remains open how these goals materialise through the new-born right. This article suggests four possible ways in which the right to data portability could unfold in the future: (i) establishing control over personal data transfers, (ii) enabling (re)use of personal data, (iii) enabling better understanding of data flows, and (iv) facilitating equality and allowing the free development of personality. Data portability could increase transparency of data processing and could allow data subjects to control their online identities. It could also be instrumental in enhancing other rights and principles, such as equality. However, the provision on data portability in the GDPR faces many legal and practical constraints. The prospects of the right will depend on regulatory interpretation and interactions with other legal areas.

Keywords
Personal data, portability, GDPR, privacy, data protection, big data

* Resident Fellow, Information Society Project, Yale University, New Haven, US; PhD Candidate, Centre for Law and Digital Technologies, Leiden University, the Netherlands, h.ursic@law.leidenuniv.nl

1 Introduction

Data portability is a fluid concept that can be used in multiple contexts and defined in various manners. One possible definition is the following: "Data portability is the ability of people to reuse data across interoperable applications."[1]

Data portability may pursue several objectives. For instance, it has been argued that data portability is inseparably tied to the goals of competition law.[2] Some recent implementations of data portability indicate that data portability can be used as a commercial strategy to please consumers.[3] Finally, data portability may pursue the goals of privacy, data protection and, as will be shown in this paper, data subjects' control over personal data.[4]

When data portability is guaranteed by law, we speak about the *right* to data portability.[5] This is the case in the EU General Data Protection Regulation, which recognises data portability as an inherent part of the EU data protection law and which has applied as of 25 May 2018.[6] As a right under data protection law, data portability's declared goal has been to strengthen individual control over data.[7] However, it remains open how this control might materialise through

---

1 DataPortability Project, http://dataportability.org (accessed 26 April 2018).

2 See for instance Maurice E Stucke and Allen P Grunes, "No Mistake About It: The Important Role of - Antitrust in the Era of Big Data" (2015) *University of Tennessee Legal Studies Research Paper*; Damien Geradin and Monika Kuschewsky, "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue" (2013) S*SRN Electronic Journa*l; Inge Graef, "Blurring Boundaries of Consumer Welfare How to Create Synergies between Competition , Consumer and Data Protection Law" in Bakhoum, Conde Gallego, Mackenordt, Surblyte (eds.), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer, forthcoming).

3 See Section 2.1.

4 Also see Alexander MacGillivray and Jay Shambaugh, "Exploring data portability" (Obama White House Archives, 30 September 2016), available at https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability (accessed 26 January 2018).

5 In this paper, a "right" is understood in Jhering's sense as a legally protected interest. See Munroe Smith, "Four German Jurists. II", (1896) 11(2) *Political Science Quarterly* 278, p. 289.

6 Art. 15 of the European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

7 Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015), p.263.

the right to data portability. Whilst there has been a lot of discussion about data portability in relation to its antitrust angle,[8] less is known about the ways in which *individuals* could make use of the right. To fill the gap, this paper discusses what sort of control and/or protection the right to data portability under the GDPR offers to data subjects. Taking into account some existing practical applications, the paper indicates four ways in which the right could unfold in the future: (i) establishing control over personal data transfers, (ii) enabling (re)use of personal data, (iii) enabling better understanding of data flows, and (iv) facilitating equality and allowing the free development of personality. Through the four gateways, data portability could increase transparency of data processing and could allow data subjects to better control their online identities. Also, the right could be instrumental in enhancing other rights and principles, such as equality. A better understanding of the gateways could thus contribute to the implementation of the new born right.

The paper starts with a short explanation of the historical development of the idea of data portability to illustrate differences in the scope and implementation of the right (Section 2). Section 3 continues with a legal analysis of the provisions in the GDPR to emphasise numerous legal and practical constraints to data portability, which put limits on the application of the right. Section 4 is the core part of the paper, investigating four gateways through which the right could enhance the specific goals of privacy, data protection law, and data subjects' control. Section 5 concludes by recognising that the four gateways face some important legal and practical boundaries, originating in the GDPR's narrowly drafted definition of data portability. As well as suggesting a more lenient interpretation of the legal provisions, the paper proposes that the use of

[8] *Supra* n. 3.

some related legal mechanisms can mitigate the downsides of the GDPR's right to data portability.

2 How and when the idea of data portability emerged

2.1 Commercial initiatives

Outside the data protection law domain, data portability as a concept emerged some time ago. For example, dataportability.org (also known as The Data Portability Project) was founded in 2007 to discuss and work on solutions to unconstraint data portability.[9] This initiative set a basis for the attempts to adopt data portability in a commercial environment.

The Data Portability Project adopted a broad definition of data portability. According to it, data portability means that "[t]he user is able to obtain her data and to transfer it to, or substitute data stored on, a compatible platform."[10] This definition can be broken down in four building blocks: free data access, open formats, platform independence, and free deletion.[11]

Following dataportability.org's initiative, some data-driven platforms have implemented voluntary solutions for export of user data they held. Among others, the project attracted some of the biggest data holders, such as Google and Facebook. For example, in 2011 Google created the "Google Takeout" tool, which allows users to export and download data from 27 of Google's products.[12] Moreover, Facebook offered a similar web-tool for downloading user information.[13] Facebook users all across the globe were (and still are) able to

---

9 Barbara Van der Auwermelen, "How to Attribute the Right to Data portability in Europe: A Comparative Analysis of Legislations" (2016) 33 (57) *Computer Law & Security Review* 57, p. 58.

10 *Supra* n. 1.

11 Todd Davies, "Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies" in Luca Maria Aiello and Daniel McFarland (eds), *Social Informatics: Proceedings of the 6th International Conference (SocInfo 2014)* (Barcelona, 2014), p. 3.

12 The tool is available at https://takeout.google.com/settings/takeout (accessed 26 January 2018).

13 The tool is available at https://www.facebook.com/help/405183566203254 (accessed 26 January 2018).

download not only the information that they have shared on their profile, but also other information that Facebook holds on them, including a log of their activity, which is visible to users when they log into their profiles, and information that is generally not visible to users, such as ads clicked on, IP addresses used for log-ins, etcetera).[14]

One common denominator of the commercial versions of data portability is that they strongly resemble the right to data access.[15] The right to access gives an individual an insight into her data but does not actually facilitate transfers to third-party providers. In fact, many commercial initiatives fail at enabling a meaningful transfer of data.[16] As shown above, data portability in its broadest sense[17] includes some extra qualities, such as platform independence, meaning that users could update their data on another platform and have the updates reflected in the platform in current use. Needless to say, platform independence has not been built into commercial data portability initiatives. This is not surprising: absolute data portability is hard to achieve, in particular in highly competitive business environments. Thus, a limited version of data portability is what major data-driven companies consider a good commercial strategy, offering consumers an extra benefit while not putting their business assets at risk.[18]

---

14 European Commission Staff, "Online Platforms Online Platforms - Accompanying the Document Communication on Online Platforms and the Digital Single Market {COM(2016) 288}" (2016), p. 37.

15 Art. 15 of the General Data Protection Regulation, *supra* n. 4. Art. 12 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

16 Sometimes willingly. See for example the discussion on portability in the House of Lords on online platforms and the EU digital single market (London, 23 November 2015), available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/oral/25076.html (accessed 26 January 2018).

17 See the definition by dataportability.org, p. 1.

18 Typically, commercial versions of data portability do no incorporate automatic, simultaneous deletion, and rarely support interoperability of formats. For more detail on this issue, see *supra* n. 16.

Google and Facebook were not the only adopters of data portability. Data portability has recently been implemented in the products of some minor software providers, for instance Project Locker[19] and CozyCloud.[20] While the former targets business users offering them a cloud repository, the latter turns to individuals, helping them handle personal data (flows). In both solutions data portability is facilitated by APIs. After users have chosen applications that they would be willing to share their data with, an API enables a connection to these applications by providing users' data.[21] This kind of data portability comes closer to the version of data portability proposed by The Data Portability Project and, as will be shown, also to the GDPR's version of the data portability right.

2.2 Regulatory initiatives

In the regulatory domain, personal data portability was introduced along with some other initiatives that promoted rights, abilities, and influence for users over their online environments and data. Building on Berners-Lee's idea of a "bill of rights" and some other calls to strengthen individual rights online, Davies included portability in his framework of digital rights.[22] Likewise, the Electronic Frontier Foundation, a privacy rights organisation, suggested that data portability should be a building block of "A Bill of Privacy Rights for Social Network Users".[23] In 2010, the US White House launched the My Data initiative with the intent to ease data access, but also to enhance data portability.[24]

---

19 http://projectlocker.com (accessed 26 January 2018).

20 https://cozy.io/en/ (accessed 26 January 2018).

21 Lachlan Urquhart, Neelima Sailaja, and Derek McAuley, "Realising the Right to Data Portability for the Domestic Internet of Things", p. 10, available at https://ssrn.com/abstract=2933448 (accessed 26 January 2018).

22 *Supra* n. 11, p. 3.

23 Kurt Opsahl, "A Bill of Privacy Rights for Social Network Users" (EFF, 19 May 2010), available at https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users (accessed 11 November 2017). Also see: Lisa A. Schmidt, "Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare" 22 (2) *Cornell Journal of Law and Public Policy* 527.

24 Kristen Honey, Phaedra Chrousos, and Tom Black, "My Data: Empowering All Americans With Personal Data Access" (Obama White House Archives, 15 March 2016), available at

In 2012, the requirement on data portability was made, for the first time, part of a data protection law. In that year the European Commission kicked off the data protection reform by publishing the draft EU General Data Protection Regulation. In relation to data portability, the EC proposal was innovative, as it suggested that data portability was introduced "…to further strengthen the control over their own data and their right of access". Thus, the proposal introduced a right with potentially far-reaching effects, but it came with little explanation regarding its implementation.

The proposed version of data portability was considered somewhat controversial. During the negotiations, EU Member States often had diverging views to what data portability was or should be.[25] At first, it was not clear from the text of the proposal whether the right was meant as a "lex social network"[26] or if it concerned every instance of data processing regardless of context, including sectors such as energy and finance.[27] Further, it was not clear whether data portability meant simultaneous access and transfer, or whether it was limited to transmission between services.[28] Similar uncertainty also arose with regards to interoperability.[29]

As shown above, data portability came to life as both controversial and promising. Now that the GDPR is applicable, the uncertainty regarding the implementation of the right to data portability is an issue of concern. Recognising

https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access (accessed 11 November 2017).

25 Materials from the GDPR negotiations in the Council available via http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf (accessed 25 January 2018).

26 A law that is primarily or even exclusively supposed to regulate social networks.

27 Kristina Irion and Giacomo Luchetta, "Online Personal Data Processing and EU Data Protection Reform" (Centre For European Policy Studies Brussels, 2013), p. 68.

28 *Supra* n. 25, p. 137. Spain, France, and Romania wanted data portability to mean the transmission of data from one controller to another. However, a majority of delegations saw the right to portability as a right to get at copy without hindrance and to transmit data from one controller to another controller.

29 Expert Group on cloud computing contracts, "Data Portability upon Switching" (2014), available at http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf (accessed 13 November 2017).

this problem, in 2016 the Article 29 Working Party issued guidelines on the right to data portability to provide some guidelines for data controllers.[30] The next section outlines the legal nature of the right under the GDPR, taking into account the Working Party's views.

3 Data portability under the GDPR

Under the GDPR, the right to portability has a twofold structure. The first component is the right of individuals to obtain a copy of their data in a structured, commonly used, and machine-readable format. The second component is that this data should be transmitted to another controller without hindrance. For the reasons which will be discussed in Section 3.4, the scope of data portability under the GDPR is very limited. As a consequence, it falls short from what The Data Portability Project considered a right to data portability.

3.1 "The … right to receive the personal data … in a structured, commonly used and machine-readable format"

In an attempt to be technologically neutral,[31] the GDPR remains silent on what exactly the terms "structured", "commonly used", and "machine-readable format" mean. Therefore, the scope of the right to data portability will be to a large extent dependent on the interpretation of these open-ended provisions. Needless to say, the format in which data is transmitted is of utmost importance for the efficiency of the right to data portability. When users receive data in generic formats, for example simply as a PDF or a zip file, they will often face difficulties with transmitting the data.[32] Hence, the right format is a pre-requisite

---

30 Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" WP 242 (April 2017), available at http://ec.europa.eu/justice/data-protection/index_en.htm (accessed 26 January 2018).

31 Technology neutrality means that the same regulatory principles should apply regardless of which technology is being used. In this way, the law does not render obsolete too quickly.

32 *Supra* n. 29.

for portability.

To explain the open-ended terms, some related legal documents could serve as a guideline. For example, in the Directive on the reuse of public sector information, "machine-readable" is defined as allowing software applications to easily identify, recognise, and extract specific data.[33] Two formats that the Article 29 Working Party explicitly recommends are CSV and XML.[34] However, even these two types of standardised formats are restricted in the sense that they do not always allow the determination of data types, primary keys,[35] possible relationships between tables (for example foreign keys) etcetera, and require additional APIs to access that information.[36]

To be "structured", data should have a specific structure, for instance it should be stored in a database or in specific files such as JSON or CSV files.[37] Structured data formats not only enhance possibilities for the reuse of datasets, but also possibilities for their coupling.[38] The latter is an integral part of large-scale data mining (data analytics).

Lastly, the data format must be "commonly used". The interpretation of "commonly used" differs from industry to industry. In the music industry, completely different formats will be used (for example the MP3[39] and AAC[40] formats) than in the health care sector (for example the standardised ODM

---

33 Recital 21 of the 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, OJ L 175, 27.6.2013.

34 *Supra* n. 30, p. 18.

35 The unique identifier of a database.

36 Darko Androcec, "Data Portability among Providers of Platform as a Service" (2013) *Research Papers Faculty Of Materials Science And Technology In Trnava, Slovak University Of Technology In Bratislava*, p. 9, available at https://www.mtf.stuba.sk/buxus/docs/doc/casopis_Vedecke_prace/32SN/002_Androcec.pdf (accessed 11 November 2017).

37 Haut Leonard et al., "D2.4 Report on the technological analysis" (EuDEco, 2016), p. 55, available at http://data-reuse.eu/wp-content/uploads/2016/06/D2.4_ReportOnTheTechnologicalAnalysis-v1_2016-02-29.pdf (accessed 26 January 2018).

38 Bart Custers and Daniel Bachlechner, "Advancing the EU Data Economy: Conditions for Realizing the Full of Potential of Data Reuse" (forthcoming 2018) *Information Policy*, p. 10.

39 MP3 is an encoding format for digital audio.

40 AAC is a proprietary encoding standard for digital audio compression. It was designed to be the successor of the MP3 format.

format for the clinical trial data[41]). In some areas, common formats are determined by formal standards. In other areas, there are no common formats at all. In such cases, the Article 29 Working Party's Guidelines recommend to use open formats.[42]

Recital 68 mentions interoperability as an additional non-mandatory requirement adding to the description of the format in Article 20. Interoperable formats enable transformation from one format to another without any loss of data. For instance, Apple's .ibooks format for ebooks can be easily transformed into the open standardised EPUB2 format.[43] This type of format interoperability should be differentiated from a perfect technical interoperability, which requires compatibility of information systems and is explicitly exempted from the data portability provision in Recital 68.[44]

3.2 "… the right to transmit those data to another controller without hindrance"

The second dimension of the right is the entitlement of individuals to transmit their personal data from one provider to another without hindrance.[45] The Article 29 Working Party translates the phrase "without hindrance" into: refraining from or slowing down access, reuse, or transmission. Examples of measures that create hindrance include lack of interoperability of formats, fees asked for delivering

41 Pascal Coorevits and others, *Electronic Health Records: New Opportunities for Clinical Research* (2013), p. 274.

42 *Supra* n. 30, p. 18.

43 *Ibid*.

44 Perfect social network interoperability (compatibility) would, for instance, enable a Google+ user to upload pictures or post messages on someone's Facebook page directly without having to create a profile on Facebook. Inge Graef, "Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union" (2015) 39 (502) *Telecommunications Policy*, pp. 14-15. In a similar sense, Ian Brown argues that interoperability actually works together, or includes, interconnectivity. Ian Brown and Chris Marsden, "Regulating Code: Towards Prosumer Law?", p. 24, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2224263 (accessed 26 January 2018).

45 Art. 20 of the GDPR, para. 1.

data, lack of access to a data format or API, deliberate obfuscation of the dataset, and excessive sectorial standardisation or accreditation demands.[46]

The Article 29 Working Party's guidance could in some cases be understood as *requiring* data controllers to ensure format interoperability. In fact, the Working Party believes that interoperability is a necessary component of a format that is standardised, commonly-used, and machine-readable. This interpretation is surprising given that Recital 68 of the GDPR explicitly states that interoperability should be *encouraged* but not made mandatory.

That said, taking such a strong position against undesirable hindrance may be critical for the success of data portability. This has been confirmed by the efforts of the EC Expert Group on cloud computing and some international standardisation bodies, who have noted a lack of interoperability and have been working on standardisation and technical solutions for data portability.[47]

3.3 "… the right to have the personal data transmitted directly from one controller to another, where technically feasible"

Data portability includes the right to have data directly transmitted from one controller to another. In line with the view of the Article 29 Working Party, the requirement can be fulfilled by making an application program interface (API) available.[48] A consortium of EU digital service providers went even further, stating that "the service provider who would not put an API to retrieve our data, while this is the most effective and cheaper to transfer data directly, would be objectively seen as trying to create friction." Besides APIs, the use of standard

46 *Supra* n. 30, p. 15.

47 *Supra* n. 29; in relation to standardisation activities of the International Organisation for Standardisation (ISO) see Irene Kamara, "Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate'" (2017) 8 (1) *European Journal of Law and Technology* 1.

48 *Supra* n. 30, p.15.

protocols has been suggested as a method of a direct transfer of data.[49]

According to the GPPR, a direct transfer of data between controllers is only required when technically feasible. What the phrase "technically feasible" actually means remains open. "Technically feasible" does not necessarily match "operationally feasible" or "economically feasible". A solution proposed by the European Banking Federation (EBF) is the following: if a data controller claims that a transfer is unfeasible, it has to prove this. If it fails to do so, portability should be facilitated.[50]

"To have data transmitted" implies a duty of data controllers to carry out the transmission. An alternative to assigning this duty to data controllers would be a third-party service based on an agency contract.[51] For example, a marketing company or a data broker would offer data subjects free products or services, a voucher or even a certain amount of money, if they authorised it to exercise their right to data portability.[52] The company (or broker) could later use this data itself, or sell it to interested companies.[53] As will be explained below, this model of data portability can be described as Data Portability as a Service (DPaaS).

3.4 The restrictive definition of the right to data portability

The limitations built into the definition of data portability indicate that the right to data portability under the GDPR is considerably restricted.

---

49 Yunfan Wang and Anuj Shah, "Supporting Data Portability in the Cloud Under the GDPR" (Carnegie Mellon University, 2018), p. 14, available at http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf (accessed 26 January 2018).

50 European Banking Federation, "European Banking Federation's Comments to the Working Party 29 Guidelines on the Right to Data Portability" (2017), p. 4, available at http://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.. .pdf (accessed 26 January 2018).

51 *Supra* n. 30, n. 4.

52 *Ibid*.

53 *Ibid*., subject to GDPR restrictions.

3.4.1 "…data provided"

The right to data portability only applies to data that has been provided to a controller by a data subject. First, this data includes personal data that the data subject has *actively* provided to the data controller.[54] Examples are email addresses, telephone numbers, preferences regarding communication etcetera, which the data subject typically communicates the first time she interacts with a data controller. Second, the right to data portability also applies to data that has been provided *passively*. Typically, this is behavioural data, which has been gathered by observing data subjects' behaviour, for example raw data processed by smart meters, activity logs, history of a website etc. *(*"observed data").[55]

However, once data has been analysed by using any sort of algorithmic techniques to draw useful insights, the results of this analysis should not be ported. It is arguable that in applying analytical techniques, data loses the direct connection with the data subject and is thus no longer considered to be "provided by them". The Article 29 Working Party refers to it as "inferred data".[56] A user's profile created by the analysis of raw smart metering is one such example. Some types of data may be between raw data and inferred data,[57] such as reputation scores that are attained by users of online marketplaces such as Airbnb. If the scores were portable, this would mean that Airbnb users would have the right to take their reviews and transfer them to a competitor, for example Couchsurfing.

The interpretation of "provided data" is one of the most disputed aspects of the GDPR's provisions on data portability, yet a critical one, as it can open up or close down the portability of a large amount of personal data. Authorities have not yet made up their minds of what the boundaries of data portability should

54 *Supra* n. 30, p. 10.
55 *Ibid*.
56 *Ibid*.
57 *Supra* n. 50, p. 4.

be. In fact, the Article 29 Working Party was criticised by the European Commission for adopting a too data subject-centric position.[58]

3.4.2 "…concerns a data subject"

The right to data portability is limited to data that "concerns a data subject". "Concerning a data subject" means that there must be a connection between the data and the identity of an individual. Consequently, anonymous data is excluded from the scope of data portability.[59] Moreover, Article 11(2) exempts a controller from complying with data subject rights when he is not able to identify the data subject. Thus, such Article 11(2) de-identified data also falls out of the scope of data portability.[60] However, if the data subject provides additional information enabling her identification, the right to data portability should again arise.[61]

Personal data records may contain multiple persons' data which are often intertwined. This may create additional difficulties in applying the right to data portability. When a data subject decides to transfer her social media data to a different platform, her decision may affect the data of a third party which is also part of the ported dataset. For example, porting photos of someone's friends from a closed social media network (for example a private Facebook group) to another which is open to public by default (for example Twitter) could infringe privacy of this person's friends. The Article 29 Working Party adopted a strict interpretation, stating that processing of such personal data by another controller should be allowed only to the extent that data is kept under the sole control of the requesting user and is only managed for purely personal or household

---

58 David Meyer, "European DPAs Mull Strategy for Tackling Uber's Data Catastrophe" (*IAPP Privacy Advisor*, 2017), available at https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/ (accessed 26 January 2018).

59 *Supra* n. 49, p. 7.

60 *Ibid*.

61 *Ibid*.

activities.[62] However, in many situations personal motives for data portability will coincide with commercial use of third party data and will likely exceed "purely personal or household activities". For example, in the case of reputation scores, an Airbnb user may want to port her data to Couchsurfing, including all the reviews that she received from Airbnb users, and may want Couchsurfing to process this data when calculating her new ratings. The Working Party's view should be taken with a grain of salt as their purpose was not to constrain data portability but rather to mitigate commercial exploitation of data portability.

3.4.3 "The processing is based on a consent … or on a contract"

Third, data portability is only applicable in cases where the legal basis for data processing is either consent or a contract (Article 20(1)(a) of the GDPR). This provision has received some criticism, since it means that a data subject would only be able to port the data that has been processed with her approval.[63] In other words, a data subject has no influence over data that has been legitimately collected and processed without her consent. For example, data processing that is based on legitimate interest of a data controller is excluded from the scope of data portability. To process behavioural data or to create consumers' profiles, controllers typically use the legal basis of legitimate interests.[64] In such cases data portability is exempted, although porting these sorts of analyses can be in individuals' interest as well.[65] Moreover, in for example the work environment,

---

62 *Ibid*.

63 Nadezha Purtova, "The Illusion of Personal Data as No One's Property" (2013) 7 *Law, Innovation, and Technology* 15. Also see Eleni Kosta and Kees Stuurman, "Technical Standards and the Draft General Data Protection Regulation" in Panagiotis Delimatsis (ed), *The Law, Economics and Politics of International Standardisation* (Cambridge University Press, 2017).

64 Gwendal Le Grand, Jules Polonetsky, and Gary LaFever, "GDPR Data Analytics Webinar Summary Three Key Points", available at https://www.anonos.com/hubfs/Whitepapers/GDPR_Data_Analytics_Webinar_Summary_Anonos.pdf (accessed 13 November 2017).

65 For some examples of data analytics based on the legitimate interest of a controller see Article 29 Data Protection Working Party, "Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC", p. 25.

the legal basis will almost never be consent but it will very often be a controller's legitimate interest.[66] Therefore, the Article 29 Working Party recommended that it will be good practice for data controllers allow data portability for data that is processed on the basis of legitimate interest.[67]

4 Data portability as an instrument of data protection through data subjects' control

As already mentioned in the introduction, the most (if not the only) plausible reason why data portability has become part of the GDPR is that it also aims at achieving the GDPR's goals of privacy and data protection. More specifically, portability of data strengthens data subjects' control over their data. Recital 68 of the GDPR sends a clear message:

> To further strengthen the *control* over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller[68]

However, the recital itself has little substance with regards to *how* data portability establishes control. Prevention of user lock-in and more consumer choice are two possible outcomes of data portability that lead to increased user control. [69] However, these goals can be to some extent achieved by the

---

66 Article 29 Working Party, "Opinion 2/2017 on Data Processing at Work" WP 249 (2017).

67 *Supra* n. 40, pp. 47-48.

68 Although Commissioner Almunia has also clearly acknowledged that data portability is also a measure of competition law. See http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm (accessed 23 January 2016).

69 See for example Kamara, *supra* n. 47, p. 11.

instruments of competition law, which prevents dominant companies from tying users to their own products, thus restricting competition.[70]

To justify its existence in EU data protection law, data portability should strive for objectives beyond those tied to competition policy.[71] Rather, data portability should pursue objectives that are instrumental to privacy and data protection. Article 20 does not articulate them clearly, but they can be distilled from the GDPR as a whole. This section suggests four objectives:

1. Establishing control over personal data transfers;
2. Establishing control over (re)uses of personal data;
3. Enabling better understanding of personal data flows and their complexity; and
4. Facilitating free development of personality and enhancing equality.

4.1. Control over personal data transfers

In a sense, data portability is a rule about data transfers. A transfer (migration) of data should happen in an organised manner, in line with data subjects' preferences. As the Article 29 Working Party explains, data portability guarantees the right to receive personal data and to process it according to the data subject's wishes.[72] For example, the data subject may opt for a more privacy-friendly service provider, for example Wire[73] instead of Skype.[74] While doing so, she might wish to ensure that all her contacts, conversation history, and chat

[70] However, it should be kept in mind that competition law measures only apply to dominant organisations. This is not that much of a problem since most often users experience the lock-in problem in the relation with companies that are dominant on the market. See *supra* n. 16.

[71] Orla Lynskey, "Aligning Data Protection Rights with Competition Law" (2017) *London School of Economics and Political Science Working Papers*, p.12.

[72] *Supra* n. 30, p. 5.

[73] Wire – a communication app offering end-to-end encrypted chats, calls, and file transfers, protected by European privacy laws.

[74] Skype is a voice over Internet Protocol (VoIP) software application used for voice, video, and instant messaging communications.

groups are transmitted to this new provider.[75]

Data "porting" can be carried out in different ways. The choice between the alternatives foreseen by the GDPR has further implications for the level of control that a data subject is able to exercise. Two possibilities are:

- A transmission of the overall dataset, or extracts of it;
- A transmission using a tool that allows extraction of relevant data.[76]

The second option gives a data subject more precise and meaningful overview and control over the information, since she may opt for portability of a limited set. As a result, the receiving controller only receives the data that is needed for a specific activity or task. As this method prevents bulk data transmission, it helps guarantee compliance with the principle of data minimisation.[77] If portability is approached in this way, then it is indeed possible to agree with the Article 29 Working Party's statement that "[d]ata portability can promote the controlled and limited sharing by users of personal data between organisations …".[78]

4.2. Control over (re)uses of data

Data portability helps data subjects not only exercise control over data transfers but also direct future uses of data. More specifically, the right to data portability has the potential to enable individuals to use data to create value.[79]

---

75 Simultaneously, a data subject will also have to make sure that his data gets deleted from the first controller's servers. Otherwise data portability will add little to actual control.

76 *Supra* n. 30, p.16.

77 Art. 6(1)(c) of the GDPR.

78 *Supra* n. 30, p.5.

79 European Data Protection Supervisor, "Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability (Opinion 7/2015)", p. 13. See also Proposal for the General Data Protection Regulation from 2012, where the possibility to use data was explicitly mentioned as one of the objectives of the right of data portability, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 26 January 2018).

For example, individuals could either use the data for their own purposes, or license the data for further use to third parties, in exchange for additional services or cash value. One viable way to do this would be to derive utility from connected (IoT) devices. For instance, athletes who track their activities with a smart watch may have trouble transmitting their data from their smart watch to the provider of a data processing service, for example Strava.[80] Data portability helps overcome the transmission hurdle. Furthermore, the athletes would get compensated for allowing their athletic performance data to be displayed and analysed on a competing platform.[81]

Data portability can only lead to control over data reuse if it is supported by functional infrastructure. For instance, by using personal data stores, privacy dashboards or other kinds of personal data management software, data subjects could hold and store the personal data and grant permission to data controllers to access and process the personal data as required.[82]

Hub of All Things is a free online tool that enables users to store and manage personal data. The hub uses "data plugs" to pull in personal data from around the internet and enables users to view their personal data and to share it with others.[83] A similar solution is the blockchain technology developed by Pikciochain, a Swiss software firm, that is intended to facilitate individual data sharing and even sale.[84] According to the founders, a special quality of Pikciochain is that all data uses are perfectly traceable, thus giving the users a

80 Strava is a website and mobile app used to log athletic activity via GPS tracking.

81 It should be noted that the European Data Protection Supervisor expressed disagreement with the possibility of monetary compensation for personal data exchange: European Data Protection Supervisor, "Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content", available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (accessed 13 November 2017).

82 *Supra* n. 30, p. 16.

83 https://hubofallthings.com (accessed 26 January 2018).

84 See *supra* n. 81, regarding the possibility of selling personal data.

better overview and control over sold, shared, or ported data.[85] Finally, the MyData initiative launched by the Finnish government is a solution that also appeals to data protection rights.[86] The aim is to provide individuals with some practical means to access, obtain, and use datasets containing their personal information, such as purchasing data, traffic data, telecommunications data, medical records, financial information and data derived from various online services and to encourage organisations holding personal data to give individuals control over this data, extending beyond their minimum legal requirements to do so.[87]

However, it should be kept in mind that many such decentralised architectures for supporting privacy self-management have failed in the past.[88] The reasons were complex, ranging from purely technical (for example network unreliability) to cognitive (for example the incorrect assumption that users were able to exercise more control than they were actually capable of).[89] Despite this, recent research has shown that modern privacy dashboards have been actually quite successful in achieving the goal of strengthening control over data flows.[90]

In spite of the myriad of options briefly described above, companies often find it difficult to convince customers to exercise their right to data portability.[91]

---

85 There are arguments against such a positive approach to the block chain technology but this discussion is out of the scope of this paper. An interested reader should be referred to: Michèle Finck, "Blockchain Regulation" *German Law Journal* (forthcoming 2018).

86 Antti Poikola, Kai Kuikkaniemi and Harri Honko, "MyData – A Nordic Model for Human-Centered Personal Data Management and Processing", available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf (accessed 1 November 2017).

87 A similar UK initiative, which has winded down in the recent months, is the "midata" project. See https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (accessed 26 January 2018).

88 Kristina Irion et al., "A Roadmap to Enhancing User Control via Privacy Dashboards" (IVIR, 2017), pp. 13-14.

89 *Ibid*.

90 *Ibid*.

91 Michael Röhsner, "Data Portability as a Service; A Legal and Normative Analysis of the Requirements under the Law of the European Union for Contracts That Authorize a Service Provider to Exercise the Right to Data Portability on Behalf of a Data Subject" (Leiden University, 2017), p. 11.

As a solution, a concept data portability as a service (DPaaS) has been proposed.[92] In a DPaaS relationship, a data subject could authorise a DPaaS-provider to exercise the right to data portability in her name and to demand the data to be sent directly to a third party or to the DPaaS-provider itself.[93] In this way, data subjects could have their data ported and transferred to a preferable provider, while businesses would benefit from access to additional data sources.[94]

One important question to answer in this regard is whether such contracts are actually allowed under EU law. One possible hesitation could be the fact that data in such contracts will be handled as a commodity, which may not be in line with the strict protection of privacy and data in the human rights laws.[95] Furthermore, a related question is if fundamental rights are transferable. The European Court of Human Rights has held that this is not the case.[96] However, exercising data portability on behalf of a data subject does not require a transfer of the right. Only data is transferred. The right to data protection remains intact, for example individuals can demand deletion of data at any time (within the legally defined limits). The authorities seem to agree with this explanation. The Article 29 Working Party even foresees such relationships to emerge in the future.[97] In the past, several Data Protection Authorities have stated that it is legal for a data subject to authorise a third party to exercise the right to access in his or

92 *Ibid*.
93 *Ibid*.
94 Also supported by *supra* n. 30, p.16.
95 For an in-depth analysis see *supra* n. 91, pp. 16-17.
96 See for example: European Court of Human Rights, *Sanles Sanles v. Spain*, App. no. 48335/99; European Court of Human Rights, *Thévenon v. France*, App. no. 2476/02; European Court of Human Rights, *Mitev v. Bulgaria*, App. no. 42758/07; European Court of Human Rights, *M.P. and Others v. Bulgaria*, App. no. 22457/08; European Court of Human Rights, *Koch v. Germany*, App. no. 497/09.
97 *Supra* n. 30, p. 19.

her name.[98] This argument can indeed be extended to all other data subject rights, including the right to data portability.[99]

However, the risk that companies would misuse this option remains present. Rather than individual control, the result would be a new form of commercial exploitation and, as a result of wide data sharing, decreased privacy protection. For example, some health care start-ups have already investigated their options under Article 20 to gain access to medical data that is typically stored at a hospital or some other health care service provider.[100] Of course, they would first need to convince data subjects to permit the transfer of their raw data. While the business case for DPaaS is solid (building new applications on vast amounts of raw data), it is not clear what benefits this would have for data subjects.

4.3. Control over complex data flows

The right to data portability could lead to better legibility of complex data flows, especially in an IoT environment. By allowing or disallowing that data to be transferred to another controller, data subjects would be able to ensure that the picture that the IoT industry has about them is complete.

At the moment, exercising the data access right can simply lead to receiving multiple pages of information.[101] With data portability, people will be able to search within and analyse the data that organisations hold about them.[102]

---

98 Austrian Data Protection Commission, Decision of the 14-12-2012, K121.897/0020-DSK/2012. See also the UK Information Commissioner's Office, "The Guide to Data Protection" (2017), p. 49, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-7.pdf (accessed 15 June 2017).

99 *Supra* n. 91, p. 18.

100 The information is based on the series of interviews conducted by the author in May 2016 with entrepreneurs from Leiden Bio Science park.

101 Loekke Moerel en Corien Prins, "Privacy for the homo digitalis - Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things", p. 65, available at http://dx.doi.org/10.2139/ssrn.2784123 (accessed 26 January 2018).

102 Jenni Tennison, "Data Portability" (Jeni's Musings, 2017), available at http://www.jenitennison.com/2017/12/26/data-portability.html (accessed 26 January 2018).

Data could be ported to data analytics services which could provide deeper insights into what information it holds. For example, individuals could examine data about particular types of activity (for example helping them to reduce their energy usage) or data that links together different types of activity (for example bringing together their transport spend with the routes that they travel).[103] Thus, the right to data portability could enable greater literacy around how data is being used.[104]

4.4. Data portability as a reflection of the right to free development of personality and equality

Data portability is a manifestation of the broader right to privacy, which is an enabler for many other rights, including the right to free development of human personality and the right to equality. [105]

First, data portability has implications for the right to free development of human personality. This can be observed in situations when data subjects have formed an entirely new personality on the internet, for example an account on a digital shopping platform that has built up a reputation and history. An example is a user's eBay reputation:

> A long-time seller on eBay has a reputation that she has built up carefully. But if she switches to the entrant, she will be a newbie again and buyers will naturally be reluctant to transact with her. But there is a ready solution: make the eBay identity and reputation portable. If I am a good seller on eBay as HotDVDBuysNow, I should be just as good on another site.[106]

---

[103] *Ibid*.

[104] *Supra* n. 21.

[105] Eva Fialová, "Data Portability and Informational Self-Determination" (2014) 8 (45) *Masaryk University Journal of Law and Technology*.

[106] Quoted from Gabriela Zanfir, "The Right to Data Portability in the Context of the EU Data Protection Reform" (2012) 6 *International Data Privacy Law*.

Indeed, on websites like eBay the concepts of digital identity and reputation are fragments of the general dimension of one's identity and reputation.[107] Both terms are strongly linked to the concept of (digital) personality. Data portability pursues the goal of free development of human personality by offering the means to achieve it, namely a technical process.[108]

Second, the EDPS suggests that data portability could also help minimise unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes.[109] Unfortunately, the EDPS did not articulate clearly how exactly data portability would achieve this. One could think of a situation in which a data subject may want to transfer data from an email service provider which uses personal data for behavioural advertising, for example Gmail, to a less intrusive one, for example Outlook. However, this still does not completely solve the problem of possible discriminatory data uses. Google would still be able to use historical data to use behavioural advertising on its Chrome browser.[110] Data portability does not mean that data is entirely removed from the first controller's server – it only means that *a copy* is transferred and reused. Only in combination with the right to erasure can portability effectively prevent data-driven decision-making that could otherwise have a negative effect on the data subject. However, using the right to data portability to send data to a third party to conduct an impartial check could decrease the risk of discrimination. In the context of profiling, portability of personal profiles to trusted third-parties could offer a solution to the lack of control over personal

---

[107] *Ibid*.

[108] See also *supra* n. 71, p. 38. It should be pointed out that portability could nevertheless be limited if third party rights would be affected.

[109] European Data Protection Supervisor, "Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy" (2014), available at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (accessed 12 November 2017).

[110] Gewirtz, David, "Your questions answered: Why I switched from Outlook to Gmail" (ZDNEt, 7 August 2014), available at http://www.zdnet.com/article/your-questions-answered-why-i-switched-from-outlook-to-gmail/ (accessed 26 January 2018)

data. These third parties would examine the profiles and determine whether the decisions made based on them were erroneous, biased, or unfair. The idea faces an important limitation: the narrow definition of the right. As data portability as a right only applies to data provided by data subject, profiled data could hardly fall within Article 20's definition. That being said, companies could allow this sort of portability voluntarily as a sign of compliance and trust.[111]

5 Conclusions

This paper examined four ways in which data portability could lead to effective individual control: (i) establishing control over personal data transfers, (ii) enabling (re)use of personal data, (iii) enabling better understanding of data flows, and (iv) facilitating equality and allowing free development of personality.

The analysis of each of these four "gateways" showed that data portability could enhance personal data protection and control over personal data. For example, data portability could increase transparency of data processing and could allow data subjects to control their online identities. Also, data portability could be instrumental to enhancing other rights and principles, such as the principle of equality. However, the effectiveness of the right depends on multiple factors. First, the language of the provision on the right to data portability in the GDPR is restrictive, because it seeks to balance competing commercial and personal interests. Section 3 has demonstrated that many types of personal data fall out of the scope of data portability. Second, portability is dependent on the ICT infrastructure. More specifically, data portability is contingent on the use of interoperable formats and systems, and on the security of those systems.[112] The

[111] Paul De Hert et al., "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" (2018) 34(2) *Computer Law & Security Review* 193.

[112] *Supra* n. 50, pp. 1-2.

success of data portability as a right will be correlated with the success of standardisation initiatives and with the robustness of information security.

To summarise, data portability as a right is very limited. At this point in time, any further regulatory changes to Article 20 are highly unlikely. To ensure that the idea of data portability survives, it will be necessary to adopt a lenient interpretation of the GDPR provisions as well as consider some alternative legal mechanisms.[113]

As already mentioned, in the area of competition law, personal data portability reinforces the goals of competition policy.[114] While the GDPR's version of the right to data portability can be only applied to personal data *provided* by an individual, competition law faces no such restriction. As a consequence, competition law can offer a remedy in situations such as the transfer of reputational profiles on sharing economy platforms, where a data subject would indeed benefit from data portability.[115] Application of competition law, however, remains contingent on the dominance of the data controller.

Furthermore, Articles 13 (2)(c) and 16(4)(b) of the proposed Directive on Digital Content could be another useful alternative.[116] The Directive addresses problems such as weakened position of consumers in the digital economy and the issue of elusive digital ownership.[117] Specifically, the directive mandates that consumers are given the option to *retrieve* their data for free when they leave a

---

[113] See for instance De Hert et al., *supra* n. 112. Due to the limited scope of the paper the implementation and enforcement aspects of the right to data portability are not further explored, although this could be interesting follow-up research.

[114] *Supra* n. 3.

[115] Aysem Diker Vanberg and Mehmet Bilal Ünver, "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?" (2017) 8 (1) *European Journal of Law and Technology*, p. 2; *supra* n. 71, p. 20.

[116] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM/2015/0634, available at http://eur-lex.europa.eu/legal- content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634 (accessed 26 January 2018).

[117] For a detailed study of this issue see Jason Schultz and Aaron Perzanowski, *The End of Ownership; Personal Property in the Digital Economy* (The MIT Press 2016).

digital service. These provisions resemble the right to portability under Art. 20 of the GDPR but are broader in scope. A retrieval is not only required with respect to personal data, but also with respect to any other content provided by the consumer and any data produced or generated through the consumer's use of the digital content.[118] This would apply, for example, to pictures uploaded by consumers, as well as to ratings they submit online.[119]

Thus, the GDPR's version of data portability is not alone on the mission to enhance data subjects' control. Some other legal domains contain similar ideas on portability that could also lead to some positive outcomes for individuals. Taking a holistic view of data portability, as well as adopting a lenient interpretation of the GDPR provisions, could be a way to make the weak right ready for the challenges of the big data era.

[118] *Supra* n. 117, Art. 13c.
[119] *Supra* n. 117, Recital 15.