
THE UNIVERSITY
*of* EDINBURGH

THE UNIVERSITY *of* EDINBURGH

# Data Portability as a New Means of Data Protection? Examining the Right to Data Portability in the EU General Data Protection Regulation

Wenlong Li

PhD in Law
The University of Edinburgh
2019

# DECLARATION

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

# LAY SUMMARY

In the digital age, internet users have generated a large amount of personal information, creative content and other forms of data. Businesses, on the other hand, heavily capitalise on collection, analysis and exchange of data for commercial insights. As the surveilling technologies deployed become increasingly revealing, intrusive and exclusive, users get the pent-up feelings that they have lost control over what they have generated online. To strengthen individual control over personal data, the new General Data Protection Regulation (GDPR), applicable in all EU Member States, introduces a new right for natural persons (in legal terms, 'data subjects') to retrieve, transmit and reuse their personal data. This new right to data portability has an immediate impact on data flow and reuse, but the contribution to the objective of data protection is not straightforward. This thesis examines how this invention furthers the objective of data protection and what is its added value to the EU data protection regime. As the right inevitably interacts with other areas of law and technology, the thesis further examines, in discrete chapters, how the new right is supplemented by recent developments in consumer protection and competition law; to what extent intellectual property rights, trade secrets and the protection of databases counteract the right's implementation; and how the right is mediated by new technological systems centred on users and by the standards of inter-operability, that is, the ability of two or more information systems to communicate with each other and exchange data.

# ABSTRACT

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect across the European Union. This new Regulation has a number of innovations, notably including a new right for the data subject to port personal data out of a processing system and reuse it elsewhere. Data portability has an immediate impact on data flows across systems and has been sought as a catalyst for competition, consumer welfare, innovation and institutional efficiency. The issue of how data portability furthers the objective of data protection appears not straightforward.

This thesis primarily examines the legitimacy, coherence and added value of the right to data portability in the EU data protection regime. In recognition of its wide-ranging implications, it also explores how the GDPR right interacts with many other areas of law and 'interfaces' with user-centric technologies devised to better protect our personal data.

The thesis is divided into six chapters. Before analysing the GDPR right, Chapter 1 first maps a wide array of similar schemes that have emerged over two decades (1995-2019), whether they be industry-initiated projects, government-led initiatives or statutory schemes. Particular attention is paid to the legacy of early attempts that predate the GDPR, as well as the recent developments in the wake of the GDPR.

Chapters 2 provides a detailed account of the right to data portability in the GDPR. It inquires whether the new right can legitimately sit within the EU data protection framework, act in harmony with other components, and bring added value to the imperative of data protection. The EU data protection regime has a dual purpose, that is, the protection of personal data and the free movement of personal data in the EU. Whereas Chapter 2 examines the right through the lens of data protection, Chapter 3 ventures to explore the right's link to the free flow of personal data. Beyond data protection, the GDPR right may also have an impact on the economic welfare of the data subject. This is especially the

case when data protection, consumer protection and competition law converge around the objective of promoting individual welfare. Chapter 3 examines whether the GDPR right may legitimately pursue consumer welfare (an overarching goal pursued by consumer protection and competition law), and how it interacts with similar schemes recently developed in those interrelated areas of law.

Chapter 4 focuses on the potential barriers to individual-led data flows, resulting from a set of information rights relating to intellectual property, trade secrets, and database protection. The extent to which the GDPR right contributes to data protection depends upon the applicability and effects of these counteracting rules. It is argued that a rough line exists between different types of data to which the data protection and information rights respectively apply. That said, grey areas do exist at the boundaries of data taxonomies, and Chapter 4 examines the rules developed for balancing the rights in conflict.

To ensure that datasets smoothly flow between systems and are well adapted to a new environment, the GDPR lays down some requirements concerning data interoperability. Chapter 5 draws knowledge from the field of data science and builds a conceptual model of interoperability to elucidate those legal requirements. Since data interoperability relies upon layers of specifications, this chapter reconstruct the EU Guidelines accordingly in order to clarify the legal issues associated with each layer of interoperability. The GDPR right's impact on data transmission and reuse is immediately noticeable; its contribution to data protection is, however, not. Basically, this right promotes data protection by channelling data into alternative systems where our data is supposedly better protected. Chapter 6 surveys the user-centric technological systems that have emerged over the last two decades (1999-2019). By revealing their attributes, development and potential interplay with the legal rights examined above, this chapter considers the extent to which a joint effort of law and technology could make a difference to our quest for data protection.

# LIST OF ABBREVIATIONS

| | |
|---|---|
| A29WP | Article 29 Working Party |
| AG | Advocate General |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| BIS | Business, Innovation and Skills |
| CFR | Charter of Fundamental Rights |
| CJEU | Court of Justice of the European Union |
| DCD | Digital Content Directive |
| DCMS | Digital, Culture, Media and Sport |
| DG | Directorate General |
| DPA | Data Protection Authority |
| DPbD | Data Protection by Design |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EU | European Union |
| EIF | European Interoperability Framework |
| FIPPs | Fair Information Practice Principles |
| FFNPD | Free Flow of Non-Personal Data |
| GDPR | General Data Protection Regulation |
| ICO | Information Commissioner's Office |
| OECD | Organisation for Economic Co-operation and Development |
| P3P | Platform for Privacy Preferences |
| PSI | Public Sector Information |
| PSD | Payment Service Directive |
| TEU | Treaty on the European Union |
| TFEU | Treaty on the Functioning of the European Union |
| US | United States |

# CONTENTS

# Introduction

This thesis looks at the right to data portability recently introduced in the General Data Protection Regulation (GDPR).[1] Obviously, the porting of data out of a processing system has an immediate impact on data flow and reuse, while inviting risks of data (in)security, breach and abuse. The intended implications for data protection seem not straightforward and hence merit a detailed examination.

## I. Data Protection in Transition: Challenges and Responses

The GDPR right was introduced at a time when the internet, big data analytics, cloud computing, and artificial intelligence, among many other technologies, have transformed many aspects of our lives. These technological advances have also brought unprecedented challenges to the legal principles developed in the last century for the protection of personal data. For instance, Zuboff notes a new logic of (resource) accumulation in the network sphere, what she calls 'surveillance capitalism'. [2] This new form of information capitalism pursues the aim of 'predicting and modifying human behaviour as a means to produce revenue and market control'.[3] Zuboff points out that many of the practices capitalising on data-driven opportunities 'challenged social norms associated with privacy and are contested as a violation of rights and laws'.[4] Cohen contends that the actors empowered by digital technologies have endeavoured to 'define and channel flows of information in ways that serve their goals'.[5] These efforts give rise to 'the prolonged and often bitter struggles over the content of the law, the design of technology, the structure of

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) OJ L 119, 4.5.2016, p. 1–88, Art 20.
[2] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75, 75. See also Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).
[3] ibid.
[4] ibid 85.
[5] Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (Yale University Press 2012) 3

information markets, and the ethics of information use'.[6] In a similar vein, Pasquale raises the concern that internet firms 'set the standard for our information economy and...have used their power to know the world of commerce ever more intimately'.[7] As a result, data is becoming 'staggering in its breadth and depth…[but] out of our reach and available only to insiders'.[8] The algorithmic methods adopted, what Pasquale describes as 'black boxes', are 'predictably biased toward informing certain hierarchies of wealth and attention'.[9]

While technologies are ever-evolving, legal norms often lag behind. After international data privacy law has weathered decades since its inception in the 1980s, Tene vividly depicts its 'midlife crisis':

*Privacy law is suffering from a midlife crisis. Despite well-recognized tectonic shifts in the socio-technological-business arena, the information privacy framework continues to stumble along like an aging protagonist in a rejuvenated cast. The framework's fundamental concepts are outdated; its goals and justifications in need of reassessment; and yet existing reform processes remain preoccupied with internal organisational measures, which yield questionable benefits to individuals. At best, the current framework strains to keep up with new developments; at worst, it has become irrelevant.*[10]

A closer look at the data protection schemes would lead to the conclusion that Tene's remarks are mostly true. The notice-and-consent model has become largely ineffective, especially in the presence of asymmetries of power and information. As Cate and Mayer-Schönberger note, individuals are often required to read 'long and complex privacy notices routinely written by lawyers for lawyers' and to take the binary choice between giving the consent or abandoning the desired service.[11] Several data protection rights are devised

[6] ibid.
[7] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (HUP 2015) 187.
[8] ibid 191.
[9] ibid.
[10] Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74(6) Ohio State Law Journal 1217, 1217.
[11] Fred H. Cate and Viktor Mayer-Schönberger, 'Tomorrow's Privacy: Notice and Consent in a World of Big Data' (2013) 3(2) International Data privacy Law 67, 67

for individuals to self-manage the data processing and the risks associated with it. However, empirical researches show that these rights are underutilised, difficult to exercise, and sometimes cause harm to the data subject exercising them.[12] Overall, the attempts at putting individuals in a position to self-manage risk are widely contested since they burden individuals with overwhelming choices and responsibilities. Whereas Solove advocates 'partial privacy self-management', [13] Blume describes strengthened consent as the inherent contradiction of European data protection law[14]. Lazaro and Le Métayer point out that individual control should not be treated merely as 'a matter of individual negotiation and autonomy', but virtually an operation dependent on an architecture of control.[15]

In view of these limitations, many scholars have been seeking solutions beyond data protection law. For instance, there is a growing body of literature on the potential interplay between data protection and competition law in the EU. [16] If the 'micro-rights' in data protection law play a limited role in

[12] Janis Wong and Tristan Henderson, 'How Portable is Portable? Exercising the GDPR's Right to Data Portability' (UbiComp/ISWC'18 Adjunct, 8–12 October 2018, Singapore). Jef Ausloos and Pierre Dewitte, 'Shattering One-way Mirrors – Data Subject Access Rights in Practice' 8(1) International Data Privacy Law 4. Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"' available at <https://marianodimartino.com/dimartino2019.pdf>accessed 5 June 2019. René Mahieu and others, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7(3) Internet Policy Review 1. Xavier Duncan L'Hoiry and Clive Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 International Data Privacy Law 190. Dominik Herrmann and Jens Lindemann, 'Obtaining Personal Data and Asking for Erasure: Do App Vendors and Website Owners Honour your Privacy Rights?' (2016) arXiv:1602.01804v2.

[13] Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1901-2.

[14] Peter Blume, 'The Inherent Contradictions in Data Protection Law' (2012) 2(1) International Data Privacy Law 26, 26.

[15] Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12(1) SCRIPTed 3, 19-20. See also Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 273.

[16] 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' (Preliminary Opinion, March 2014). European Data Protection Supervisor, 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (Opinion 8/2016, 23 September 2016). See also 'Symposium on Data Protection and Competition Law' (International Data Privacy Law, August 2018) available at <https://academic.oup.com/idpl/issue/8/3>accessed 7 June 2019.

rebalancing the power between individuals and businesses, competition law could address the asymmetries of power in a more holistic manner. Scholars in both the US[17] and EU[18] have also attempted to re-conceptualise data protection in the terms of data ownership and draw lessons from traditional property principles. Because of the ever-evolving risks arising from data processing, efforts have been made to prevent certain severe harms by imposing further restrictions on data processing.[19] Out of legal thinking, some have resorted to technological design that ensures the protection of data privacy at the beginning of the infrastructure design.[20]

The GDPR is a hybrid model that incorporates many of the approaches mentioned above. As the European Data Protection Supervisor puts it, this Regulation addresses covert profiling by enhanced transparency, facilitates data sharing through user control, minimises risks by Privacy by Design, and ensures overall compliance by accountability.[21] While these approaches are equally important to ensure a high level of data protection, this thesis primarily looks at data portability as a new means of data protection. Where relevant, it reveals how the right to data portability in the GDPR interacts with EU rules on competition, consumer protection, property (rights) and technological design.

## II. Understanding Data Portability

At the first Hackers Conference in 1984, a visionary American writer, Stewart Brand, once told Steve Wosniak, the co-founder of Apple, that

*On the one hand information wants to be expensive, because it's so valuable.*

[17] For instance, see 'Symposium: Cyberspace and Privacy: A New Legal Paradigm?' (Stanford Law Review, May 2000), available at <https://www.jstor.org/stable/i252780>accessed 7 June 2019.
[18] Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2012). Christopher Rees, 'Tomorrow's Privacy: Personal Information as Property' (2013) 3(4) International Data Privacy Law 220.
[19] Fred H. Cate, 'The Failure of Fair Information Practice Principles' in Jane Winn (ed), *Consumer Protection in the Age of the Information Economy* (Routledge 2006) 341.
[20] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (HUP 2018). Claudia Diaz, Omer Tene and Seda Gürses, 'Hero or Villain: The Data Controller in Privacy Law and Technologies' (2013) 74 Ohio State Law Journal 923.
[21] European Data Protection Supervisor, 'Opinion on Meeting the Challenges of Big Data: A Call for Transparency, User control, Data Protection by Design and Accountability (Opinion 7/2015, 19 November 2015).

*The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So, you have these two fighting against each other.*

These lines became widely known in the following decades when, precisely as Brand had foreseen, there was an exponential increase of data flows among businesses. There could be many interpretations of Brand's vision, but that the value of data determines its mobility stands out among others.

When the internet was born in the 1990s, data portability was still a technical challenge. Many computer scientists endeavoured to develop conceptual models, specifications and standards to enable the data flow between heterogeneous information systems.[22] At the beginning of the 21st century, many of the technical problems about moving data between information systems had been fully resolved. Further, a wide array of new technologies has fundamentally changed the purposes, methods and direction of information flows. For instance, the rise of web 2.0 (*i.e.* a social web featuring user-generated content) and cloud computing (*i.e.* a network of remote servers hosted on the internet) increase the need of data portability respectively for individuals and businesses. With the advent of big data analytics, data has become a type of reusable resource and data processing a distinct kind of service, *i.e.,* data as a service (DaaS). The increasing use of Application Programming Interface (*i.e.* a special software allowing for communication between systems and real-time data exchange) provides for real-time data exchange and data-driven innovation. In parallel, new technological systems are being built to put individuals at the centre of data management and give them full control over their personal data. Beyond the private sector, interoperability and data portability have been sought by public authorities to improve institutional efficiency.

[22] Peter Wegner, 'Interoperability' (1996) 28(1) ACM Computing Surveys 285, 285. Tim Berners-Lee, James Hendler and Ora Laasila, 'The Semantic Web' (Scientific American, May 2001) available at <https://www.scientificamerican.com/article/the-semantic-web>accessed 30 November 2018. Kim H. Veltman, 'Syntactic and Semantic Interoperability: New Approaches to Knowledge and the Semantic Web' (2001) 7(1) New Review of Information Networking 159.

As technology keeps evolving, the essence of data portability is changing over time. The perception of data portability varies from context to context, and there exists no one-size-fits-all definition. Perhaps the broadest one may come from the Internet Association, a US-based industry trade group, that data portability is 'a wide array of practices, from e-commerce exchanges of PII between private sector buyers, sellers and payment platforms to cyber threat information exchange between the public and private sectors'.[23] Apparently, this definition virtually covers data flows in all possible contexts. In contrast, other definitions have been developed primarily in a business-to-consumer context. The White House's Office of Science and Technology Policy (OSTP) sees it as 'the ability to download the information that a service stores for or about an individual…and to enjoy the convenience of keeping our data online, and the ability to gain access to it and use it how we wish'.[24] Lynskey refers to data portability as 'providing individuals with the opportunity to obtain access to their own information in order to use it for further purposes'.[25] From a technical perspective, Petcu defines data portability as 'the ability of a customer (individual or organisation) to retrieve application data from one provider and import it into an equivalent application hosted by another provider'.[26]

Clearly, existing definitions of data portability are diverse, fragmented and inconsistent. The difficulties in achieving a shared definition result, it is argued, from several contingent factors:

1. Scope and types of data, *e.g.* personal data, usage data, consumer data

[23] White House Office of Science and Technology Policy, 'Request for Information Regarding Data Portability' (White House Archive, 10 January 2017) 47.
[24] Alexander Macgillivray and Jay Shambaugh, 'Exploring Data Portability' (White House Archive, 30 September 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability>accessed 17 December 2018.
[25] Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 6 European Law Review 793, 796.
[26] Dana Petcu, 'Portability and Interoperability between Clouds: Challenges and Case Study' (2011), in Witold Abramowicz and others (ed.), *Towards a Service-based Internet* (Springer 2011) 62, 67.

2. Stakeholders concerned, *e.g.* business, public authorities, individuals
3. Methods, *e.g.* data export/download, data transfer, automatic data exchange (through APIs)
4. Purposes, *e.g.* competition, consumer welfare, innovation, institutional efficiency
5. Level of Intervention, *e.g.* self-regulatory, co-regulatory, statutory

These factors identified are interrelated with each other. For instance, the purpose of data portability dictates the scope of data concerned, the optimal method possible, as well as the level of intervention required. Concerning the stakeholders involved, this thesis primarily looks at the data flows from commercial entities to individuals. It will be shown that lessons can nevertheless be drawn from the public sector. The GDPR right to data portability applies only to a limited scope of data, defined as any information relating to and provided by an identified or identifiable natural person ('data subject').[27] That said, the scope of portable data has been extended by some recent EU instruments to 'non-personal data'.[28]

With regard to the method of delivery, this thesis provides a typology of data portability comprising three categories:

1. data (information) access for switching
2. data portability as switching
3. data exchange without the need for switching

First, it should be noted that data portability has for a long time been considered necessary to allow switching from one service provider to another. In this respect, the porting of data refers to access to useful information in order to find the best deal. The information is primarily concerned with transaction, usage and consumption, with which consumers can make better decisions.

Second, data conveys much more than plain information. As added value can be extracted using advanced processing techniques, data becomes a reusable

[27] GDPR, Art 4(1) and 20(1).
[28] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303, 28.11.2018, p. 59–68, Art 6(1).

resource and data processing a distinct type of service (known as data-as-a-service). In this case, the porting of data equates with the switching of service.

Last, the increased use of APIs to connect different systems prompts a rethinking of data portability, and in particular, its historical link with the need for switching. Since data can be 'queried' while still residing in the same system, there is no need to move data out of a system for reuse purposes. From a technical perspective, this not only saves bandwidth but ensures that the exchanged data is up-to-date.[29] Users might have second thoughts about switching if they are allowed to multi-home, that is, to use numerous services of complementary or equivalent functionality at the same time.

## III. Data Portability as a New Means of Data Protection

Over the two decades, data portability has been sought for competition, consumer welfare, innovation, and institutional efficiency, etc. The marriage of data protection and data portability is indeed a recent innovation. This thesis primarily looks at how, and to what extent, the right to data portability adds to the new EU data protection regime while serving the objective of data protection.

The recital 68 of the GDPR states that the right to data portability is devised to strengthen individual control over personal data.[30] The full text of Art 20 concerning the right to data portability is provided in the following:

> 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:

[29] Open Data Handbook: Glossary, available at <http://opendatahandbook.org/glossary/en>accessed 5 December 2018.
[30] GDPR, recital 68.

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.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

In comparison to the original version proposed by the European Commission, this right is much more comprehensive and complicated, with the objective, conditions/exceptions, and the scope of application significantly altered.[31] The bulk of this thesis will look at these provisions to unfold the right's contribution to the protection of personal data.

The recent link between data protection and data portability has been partially addressed by earlier literature. When the GDPR proposal was released around the 2010s, many competition law scholars first spilt ink on this new legal invention in the EU data protection regime.[32] Given the right's contested impact on data protection and potential disruption to the market, they propose that the GDPR right should be aligned with the logic of competition.[33] In

[31] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, Art 18. See also Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335.
[32] Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335. Graef and others, 'Putting the Right to Data Portability into A Competition Law Perspective' (2013) Law Journal of the Higher School of Economics 53. Barbara Engels, 'Data Portability among Online Platforms' (2016) 5(2) Internet Policy Review 1, 10.
[33] ibid.

response, data protection scholars made a case for the right on the grounds of fundamental rights.[34]

These accounts provide some context for situating the new right at the intersection of EU law, but do not give a full account of the right's multi-faceted, technology-mediated contribution to the goal of data protection. Further, the extent to which the right is being affected by the protection of intellectual property, trade secrets and database making, as well as by technical challenges to data interoperability, remain understated. From the outset, the elusive nature of the right to data portability raises concerns about the right's consistency with the objectives and instruments of data protection, and its external interplay with competition and consumer welfare. Further, the right is largely built upon several technical and legal conditions; its contribution is likely to be reduced by potential technical, legal and practical hurdles. Eventually, the right-based data portability is operated on the basis that data subjects use it actively and effectively. Given the right's apparent complexities, it is reasonable to assume that data subjects need further assistance to use it wisely.

## IV. Structure of the Thesis

This thesis deals with these thorny issues through six chapters. Chapter 1 puts data portability in the self-regulatory, co-regulatory and statutory contexts. To ease the understanding of data portability and its normative values, it maps the grassroots efforts, industry-initiated projects, government-led initiatives as well as legal regimes in the US, UK and EU. Before introducing the GDPR right to data portability, this chapter explains the legacy of early schemes as well as recent developments in the wake of the GDPR.

[34] Gabriela Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 2(3) International Data Privacy Law 149. Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-determination off the Table, and Back on Again?' (2014) 30(1) Computer Law & Security Review 6. Lynskey (n 25) 811.

Chapter 2 provides a detailed account of the right to data portability recently introduced in the EU data protection regime. To justify it on the grounds of data protection, this chapter traces its conceptual origin, the right to informational self-determination, in German constitutional jurisprudence. Apart from the legitimacy issue, Chapter 2 also examines the new right's added value to EU data protection law, compatibility with existing rights of access and to erasure, as well as the interplay with the new principle of data protection by design and by default.

Beyond data protection, chapter 3 focuses on the GDPR right's externalities. The right was introduced at a time of EU law convergence when data protection, consumer protection and competition law bled into each other. New schemes similar to the GDPR right to data portability have been introduced, making the legal landscape diverse, complex and fragmented. Chapter 3 inquires whether the GDPR right can be aligned with consumer welfare, an overarching value both consumer protection and competition law promote. Further, it examines to what extent the GDPR right could be used to facilitate switching or alleviate lock-in, in tandem with new schemes introduced in consumer protection and competition law.

Chapter 4 looks at the right's interplay with intellectual property rights, trade secrets and database protection. These 'information rights' often constitute barriers to individual access to personal data, and would exert an influence on the legal rights concerning data portability. It is argued that data taxonomies could intermittently avoid the conflict of rights by drawing a line between different categories of data; the rules for balancing the rights are still needed in the grey areas where conflict is inevitable to occur.

Chapter 5 goes beyond the legal context and draws on the knowledge of data science to elucidate the technical specifications of data portability required by law. To ensure that personal data can be seamlessly transmitted and readapted to the new environment, guidelines from data protection authorities

would play a crucial role in facilitating interoperability. As interoperability is construed by multiple layers of technical specifications, this chapter reconstructs the EU guidelines in this layered fashion, and explores several legal issues associated with each layer of interoperability. These issues are concerned with, for instance, the leeway to find the optimal method, the use of proprietary formats and the provision of metadata.

The last chapter surveys a selection of user-centric systems that have emerged over two decades (1999-2019). These systems represent the future of data protection but are struggling to increase user awareness and adoption. Since the legal rights to data portability connect well with these user-centric systems, this chapter explores whether the combined effort of law and technology would bring better protection and management to us.

## V. Methodology and Methods

This thesis involves library-based, legal research. It considers legal doctrine, case-law and statutory measures as primary sources. Background policy papers as well as academic commentary and analysis are used as secondary sources. To be specific, the majority of books, journal articles and reports are obtained from the University of Edinburgh's libraries, the National Library of Scotland, and the UK's Interlibrary Loans Scheme. The thesis has a moderate level of engagement with data science but adds no original contribution to it.

At EU level, all EU instruments are accessible through the official website EUR-lex. The CJEU caselaw is accessed via the website CURIA as well as Westlaw. Reports, Guidelines and Opinions from EU authorities (such as the Article 29 Working Party, European Data Protection Supervisor, European Data Protection Board) are publicly available on their official websites. At UK level, reports from government bodies, such as the Information Commissioner's Office, Competition and Markets Authority, Department for Digital, Culture, Media and Sport, Department for Business, Innovation & Skills, are accessible on the internet. Reports from other organisations, such as the

OECD, World Economic Forum, CtrlShift, can be found on their websites as well.

For this research, two requests were made to the European Commission for access to EU documents. On 30 March 2018, the first request was made for access to public responses to the Article 29 Working Party's consultation on the Guidelines concerning the right to data portability, issued on 13 December 2016.[35] The second request, made on 9 December 2018, concerns legislative documents on the evolution of the right to data portability during the passage of the GDPR.[36]

To have a direct view of personal data obtainable through the GDPR, ten data portability requests were made on 25 March 2018, respectively to Facebook, Instagram, Twitter, WeChat, Amazon, Google, Apple, University of Edinburgh, Runkeeper (fitness tracker) and UK Border Agency for a copy of my personal data. This moderate sample was used for inspiration only and does not make any empirical contribution to this thesis.

[35] Request for Access to EU Documents, registered on 20 March 2018, Ref GestDem No 2018/1669.
[36] Request for Access to EU Documents, registered on 9 December 2018, Ref GestDem No 2018/6570.

# Chapter 1 Data Portability in Context

## Introduction

Since the turn of the century, a wide array of initiatives, policies and laws have emerged around the world, facilitating data flows from organisations to individuals. These schemes have different objectives, methods and scope of application; ostensibly, they have inspired the later development of legal regimes relating to data portability in the European Union (EU) and beyond.

To foster a richer, up-to-date understanding of data portability and its multifaceted value, this chapter maps the industry-initiated projects, government-led initiatives and legal regimes in the US, UK and EU. It aims to showcase the legacy of early schemes as well as the recent developments in the wake of the GDPR. The right to data portability, along with its history, essence and added value, will be detailed in Chapter 2.

The structure of this chapter is as follows. Prior to any solid scheme of data portability, there emerged a wave of calls for data portability on the internet. This chapter first provides a brief account of these grassroots efforts to express the need for data portability. Further, it respectively maps the self-regulatory, co-regulatory, and regulatory schemes concerning data portability emerged within nearly two decades (2000-2019). The chapter ends with reflections on the evolving nature of data portability, as well as the trajectory of policy- and law-making in the EU.

## I. Grassroots Efforts to Promote Data Portability

Around the 2010s, a number of proposals (in the form of Bill of Rights) emerged on the internet, calling for data ownership, control and digital rights. Ostensibly, the first 'Bill of Rights' was drafted by Joseph Smarr and others as part of their project 'Open Social Web'.[37] It lays down a number of 'fundamental

[37] Joseph Smarr and others, 'A Bill of Rights for Users of the Social Web' (Open Social Web, September 2007) available at <https://domainmarketresearch.com/?page_id=359>accessed 16 December 2018.

rights' and, among them, data portability is understood as 'the freedom to grant persistent access to their personal information to trusted external sites'.[38] Users should be able to use 'persistent URL, API token and open formats...to syndicate their profile data, friend lists and streams of activities on social networks'.[39] O'Heal contends that this 'fundamental right' was to address the issue of (the lack of) interoperability between social network sites.[40] If these sites do not interoperate, users cannot switch between, or co-exist on, them.

Three years later, the Electronic Frontier Foundation (EFF), a civil liberty non-profit organisation co-founded by John Perry Barlow, released its Bill of Privacy Rights for Social Network Users in May 2010.[41] Opsahl argues that one way for users to protect their privacy is to 'leave a social network service that does not sufficiently protect it'.[42] The proposed right to leave consists of two parts: (1) delete data and account from a social network service and (2) take the data away from that service and move it to a new one. As an increasing volume of data is generated on social media, constituting high switching costs, such a right to leave is crucial for consumers to combat lock-in.

In the same year, another 'Social Network Users Bill of Right' was widely discussed online as a response to the privacy scandals over several major social networking service providers.[43] Gagnier, the drafter of that Bill of Rights, argues for data portability as a fundamental right to be respected by service providers in their Terms of Service, Privacy Policies, or any other documents implementing their systems.[44]

---

[38] ibid.
[39] ibid.
[40] Steve O'Hear, 'A Bill of Rights for Users of the Social Web' (ZDNet, 6 September 2007) available at <https://www.zdnet.com/article/a-bill-of-rights-for-users-of-the-social-web>accessed 7 December 2018.
[41] 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 16 December 2018.
[42] ibid.
[43] Christina Gagnier, 'A Social Network Users' Bill of Rights: "You" Must Decide' (2011) available at <https://www.w3.org/2011/track-privacy/papers/GagnierMargossian.pdf>accessed 16 December 2018.
[44] ibid.

To note, there are numerous other Bill of Rights online calling for data flows from commercial entities to individuals.[45] These grassroots efforts do not have any legal effect but have clearly expressed the need for data portability and its potential impact on privacy, switching, lock-in, data transmission and reuse. Ostensibly, these efforts paved the way for the US Consumer Bill of Rights, the MyData schemes in the US, and the midata scheme in the UK.

## II. Self-regulation: Business Value of Data Portability

Before policymakers and legislators around the world address the issue of data portability, it was primarily industrial-led projects that promote the flows of data from businesses to individuals. Indeed, businesses generally do not have an incentive to share databases with competitors, governments and even users. For different reasons, there are still few companies proactively embracing data portability of their own accord. To note, there was a data portability project established as early as 2007.[46] With an aim to 'put existing technologies, techniques, policies and initiatives in context', this project did not produce any actual product or service nonetheless.[47]

---

[45] Parker Higgins, 'Mobile User Privacy Bill of Rights' (EFF, 2 March 2012) available at <https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights>accessed 16 December 2018. John Battelle, 'The Data Bill of Rights' (Battelle Media, 25 April 2007) available at <https://battellemedia.com/archives/2007/04/the_data_bill_of_rights>accessed 16 December 2018. Jeff Jarvis. 'My Cyberspace Bill of Rights' (The Guardian, 29 March 2010) available at <https://www.theguardian.com/commentisfree/2010/mar/29/internet-censorship-cyberspace-bill-of-rights >accessed 16 December 2018. Mark Sullivan, 'A Bill of Rights for Facebook Users' (PC World, 20 May 2010) available at <https://www.pcworld.com/article/196798/BOR.html>accessed 16 December 2018. Jack Lerner and Lisa Borodkin, 'We, the users - Facebook users' Bill of Rights' (SF Gate, 21 May 2010) available at <https://www.sfgate.com/opinion/article/We-the-users-Facebook-users-Bill-of-Rights-3263476.php>accessed 16 December 2018. Bruce Sterling, 'The Ello Bill Of Rights for Social Network Users' (WIRED, 7 January 2015) available at <https://www.wired.com/beyond-the-beyond/2015/07/ello-bill-rights-social-network-users>accessed 12 December 2018. Duncan Work, 'Call for A Social Networking Bill of Rights' (Planetwork Journal, July 2004) available at <http://planetwork.net/journal>accessed 16 December 2018.

[46] Data Portability Project, available at <http://dataportability.org>accessed 4 June 2019. See also Crunchbase, Overview of the Data Portability Project, available at<https://www.crunchbase.com/organization/dataportability>accessed 16 December 2018.

[47] ibid.

### 1. Google Takeout: ‘Liberating’ Google Products

Google Takeout is the first self-led attempt in the industry at enabling data portability for users. The Data Liberation Front (DLF), an engineering team in Google, was established in 2011 for ‘liberating’ Google products. In 2011, the DLF released the first product called Google Takeout, which allows Google users to export their data in portable and open formats.[48] Starting from only a few products (Google Buzz, Contacts and Picasa), the DLF has gradually expanded the scope of liberated products over the years. Now, Google allows for data exports from all of its 50+ services.[49]

### 2. Evernote: Three Laws of Data Protection

Evernote has been a perennial advocate of data portability. Phil Libin, the previous CEO of Evernote, supports data portability as a spur for the company: ‘our philosophy is that by making it possible for you to leave at any time, we are forever motivated and build great things so that you will want to stay’.[50] In 2014, Libin expressed the Evernote’s Three Laws of Data Protection, according to which data held by Evernote are protected, portable and ‘owned’ by the users. The third ‘law’ concerns data portability, and Evernote aims to make data portable and allowing the users to switch. The desktop version of Evernote supports data exports in HTML/XML formats and, as Libin promised, ‘a full, free API’ is deployed for this purpose.[51]

---

[48] Brian Fitzpatrick, ‘The Data Liberation Front Delivers Google Takeout’ (Data Liberation Blog, 28 June 2011) available at <http://dataliberation.blogspot.com/2011/06/data-liberation-front-delivers-google.html>accessed 20 December 2018.

[49] Google Account, ‘Download Your Data’ available at <https://takeout.google.com/settings/takeout>accessed 20 December 2018. Some of these services are no longer available due to strategic changes. For instance, Google has decided to shut down its failing social networking service, Google+, after a data breach incident in December 2018. Anthony Cuthbertson, 'Google+ to Shut Down Early after Data from 52 Million Users Exposed' (Independent, 11 December 2018) available at <https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-plus-shut-down-date-bug-personal-data-breach-alphabet-inc-a8677296.html>accessed 20 December 2018.

[50] Phil Libin, ‘Evernote’s Three Laws of Data Protection’ (Evernote Blog, 3 June 2014) available at <https://evernote.com/blog/three-laws-of-data-protection-update>accessed 20 December 2018.

[51] ibid.

### 3. Data Transfer Project

Google's DLF is now in collaboration with the engineering teams from Facebook, Twitter and Microsoft. In July 2018, they announced the Data Transfer Project (DLF), an open-source, service-to-service data portability framework.[52] Building upon interoperability between these popular platforms, the DTP aims to support seamless, direct, user-initiated data flows through Application Programming Interfaces (API).[53] According to the DTP whitepaper, the framework is open to other service providers as well, and the DTP aims to cultivate an open ecosystem.[54]

What can be gleaned from these self-led projects is that popular platforms seek data portability for varied reasons. Whereas Google's lead is consistent with its openness policy,[55] other platforms joined this community mostly out of legal pressure[56]. In the case of Evernote, most contents are generated by users, and individual rights typically subsist on them. The Evernote's first law concerning ownership seems not entirely genuine, given that users are required to permit Evernote to 'back data up, send them to a network and share it with business partners'.[57]

## III. Private-Public Partnership: The Role of Public Policy

At national policy level, both the US and UK Governments led the development of data portability policy through public-private partnerships. The Mydata schemes, led by the Obama administration, is ostensibly the first public policy

[52] 'Data Transfer Project (DTP): About Us' available at <https://datatransferproject.dev>accessed 20 December 2018.
[53] Data Transfer Project, 'Overview and Fundamentals' (DTP Whitepaper, 20 July 2018)
[54] DTP (n 16).
[55] Scott Carey, 'How Google Decides to Open Source its Technology: Two Google Executives Shine a Light on the Tech Giant's Open Source Strategy' (Computer World, 6 August 2018) available at <https://www.computerworld.com.au/article/644791/how-google-decides-open-source-its-technology/ >accessed 2 June 2019.
[56] Ellen Tannam, 'Tech Titans Join Forces for the Data Transfer Project – so How Will it Work?' (Silicon Republic, 20 July 2018) available at <https://www.siliconrepublic.com/enterprise/data-transfer-project-explained>accessed 2 June 2019.
[57] ibid.

concerning data portability. Shortly after its inception, a programme of the same name (which later changed its name to midata) emerged in the UK.

### 1. Mydata: The First Data Portability Policy across the Globe

In 2010, the Obama administration pioneered a package of data portability initiatives called 'MyData', which cover a few sectors such as health, energy, finance, education and social security.[58] The US policymakers explained that these initiatives responded to the US consumers' struggles to get access to their own information.[59] In these initiatives, the federal government provides support for developing interoperability, security and access, whereas businesses respond with the efforts to produce industry-wide standards.

In January 2010, 'Blue Button' was launched in the healthcare sector to facilitate patients' access to medical records. This initiative aims to help patients 'track their health, correct errors, be more effective caregivers, and better facilitate information sharing between doctors, specialists and their family'.[60] Building upon Blue Button, the Precision Medicine Initiative aims to further facilitate data access for scientific research purposes.[61] Green Button is an initiative in the utility sector that facilitates access to usage data.[62] The US consumers are empowered with access to their data to 'better understand their energy consumption patterns and make smarter decisions'.[63] Beyond

[58] Kristen Honey, Phaedra Chrousos, and Tom Black, 'My Data: Empowering All Americans with Personal Data Access' (White House Archive, 15 March 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access>accessed 17 December 2018.
[59] ibid.
[60] ibid.
[61] The White House Office of the Press Secretary, 'Factsheet: President Obama's Precision Medicine Initiative' (White House Archive, 30 January 2015) available at <https://obamawhitehouse.archives.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative>accessed 17 December 2018.
[62] 'What is Green Button' (Energy.gov) available at <https://www.energy.gov/data/green-button>accessed 17 December 2018. See also Aneesh Chopra, 'Modelling a Green Energy Challenge after a Blue Button' (White House Archive, 15 September 2011) available at <https://obamawhitehouse.archives.gov/blog/2011/09/15/modeling-green-energy-challenge-after-blue-button> accessed 17 December 2018.
[63] Kristen Honey, Phaedra Chrousos, and Tom Black, 'My Data: Empowering All Americans with Personal Data Access' (White House Archive, 15 March 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access>accessed 17 December 2018.

individual wellbeing, Green Button plays a role in 'facilitating virtual edits to identify inefficiencies' and translating consumer empowerment into 'cost saving and cleaner environment'.[64] MyStudentData is a student-empowering initiative in the education sector. It assists the students with their choice for paying off debt or choosing where to attend school.[65] Students in the US are entitled to retrieve their data (*e.g.* loan, grant, enrolment and overpayment information) from the National Student Loan Data System, in a 'simple, machine-readable and plain-text file'.[66] Last, MySocialSecurity accounts are provided to citizens for better planning their retirement.[67] They can download a copy of the benefit statement and share it with their financial advisors or analyse it using a software.

Given the progress made by Mydata schemes, the White House Office of Science and Technology Policy (OSTP) conducted an official Request for Information (RFI) in September 2016, the time when the EU General Data Protection Regulation had just been approved. The RFI raised a few general questions concerning data portability, notably including:[68]

1. The potential benefits and drawbacks of data portability
2. The industries that would most benefit or be harmed
3. The specific steps for the US federal government, private companies and others to take to encourage or require greater data portability
4. Best practices in implementing data portability

In the summary of results released in early 2017, the OSTP acknowledges that the EU and other countries in the world are ensuring data portability through legislation. In the US, the Obama administration had attempted to put data

[64] ibid. Honey and others (n 22).
[65] ibid.
[66] 'The MyStudentData Download Function Allows You to Access Your Federal Student Aid Information or Your FAFSA Information in A Plain Text File', available at <https://studentaid.ed.gov/sa/resources/mystudentdata-download#what-is-mystudentdata>accessed 17 December 2018.
[67] Honey and others (n 22).
[68] Alexander Macgillivray and Jay Shambaugh, 'Exploring Data Portability' (White House Archive, 30 September 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability>accessed 17 December 2018.

portability in legislation. Proposed in 2015[69], the US Consumer Privacy Bill of Rights Act has ostensibly floundered after the General Election in 2016.[70]

## 2. Midata: Echoes at the Other Side of the Atlantic?

As part of the Consumer Empowerment Strategy, the UK's midata scheme gives consumers access to their transaction data in an 'electronic, portable and safe' way.[71] Unlike its US counterparts, which are part of the US Consumer Privacy Framework, the UK's midata is by nature market-oriented, sector-specific, with a focus on micro-, small-, and medium-sized enterprises. It adopts a sectoral approach and focuses upon 'core sectors' (*i.e.* energy, telecommunication and banking) in which data portability is mostly needed.[72] In 2013, the Current Account Switch Guarantee (CASG) was introduced to boost competition among banks and help consumers switch within seven days.[73] In the energy sector, an agreement exists in the seven largest energy suppliers concerning the provision of midata files to consumers.[74] Machine-

[69] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (White House Archive) available at <https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>accessed 17 December 2018.

[70] James Denvil and Patrick Kane, 'Insights on the Consumer Privacy Bill of Rights Act of 2015' (Hogan Lovells Chronicle of Data Protection, 3 March 2015) available at <https://www.hldataprotection.com/2015/03/articles/consumer-privacy/insights-on-the-consumer-privacy-bill-of-rights-act-of-2015>accessed 17 December 2018. Adam Chernichaw, 'White House Re-Introduces Consumer Privacy Bill of Rights Act' (White & Case, 8 April 2015) available at <https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act>accessed 17 December 2018.

[71] BIS, 'Government Response to 2012 Consultation' (GOV.UK, 27 July 2012) 8, available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43392/12-1283-midata-government-response-to-2012-consultation.pdf>accessed 8 February 2018.

[72] To note, midata applies only to the UK's private sector. A separate agenda called Transparency and Open Data Agenda promotes data access and portability in the public sector. See Department for Work and Pensions, 'Transparency and Open Data' (GOV.UK, 10 April 2013) available at <https://www.gov.uk/government/publications/transparency-and-open-data>accessed 2 June 2019.

[73] HM Treasury and The Rt Hon George Osborne, 'Bank Account Switching Service Set to Launch' (GOV.UK, 10 September 2013) available at <https://www.gov.uk/government/news/bank-account-switching-service-set-to-launch>accessed 22 December 2018. To note, the UK's Independent Commission of Banking (ICB) had discussed account number portability, an alternative to the CASG, that allows the customer to keep his or her sort code and account number when switching banks. While account number portability has apparent advantages, the ICB nevertheless favours the cost-saving CASG. It states in the banking report that should the CASG do not achieve the aim of effective switching, full account number portability would then be considered. See Independent Commission on Banking (ICB), 'Independent Commission on Banking: Final Report' (GOV.UK,12 September 2011) 17.

[74] BIS, 'Switching Principles: Call for Evidence' (GOV.UK, 22 October 2015) 39.

readable images, such as QR codes or two-dimensional codes, are provided to consumers for accessing their energy data.[75] In addition, the midata Innovation Lab (mIL) is in collaboration with the industry to develop applications for consumers.[76] In July 2015, the UK's Competition and Markets Authority (CMA) launched reform in the energy sector, proposing changes such as increased access to customer data by Price Comparison Websites (PCW) and access to more types of utility data.[77] The BIS notes there wasn't any equivalent scheme enabling consumers to obtain and reuse data in the telecommunication sector.[78] Apart from that, Ofcom took the effort to enable number portability, that is, the ability of a consumer to retain his or her telephone number when changing mobile network operators.[79]

In 2013, the Enterprise and Regulatory Reform Act (ERRA) was enacted to legislative a power to give midata a statutory footing.[80] The Act opens up the possibility of extending midata to non-core sectors but set 'a high bar' for doing so.[81] The UK Government believes that data portability is only needed where[82]

1. The market is not working well for consumers (*e.g.* consumers find it challenging to make the right choice)
2. There tends to be a one-to-one, long term relationship between the business and the customer, with a stream of ongoing transactions
3. Consumer engagement is currently limited (*e.g.* low levels of switching between tariffs, account types or providers)
4. The sector does not voluntarily provide transaction/consumption data to customers at their request in portable electronic format

[75] ibid.
[76] Emily Bater, 'Midata - Making Comparison Better' (GoCompare) available at <https://www.gocompare.com/money/midata>accessed 22 December 2018.
[77] Competition and Markets Authority, 'CMA Sets out Case for Energy Market Reform' (GOV.UK, 7 July 2015) available at<https://www.gov.uk/government/news/cma-sets-out-case-for-energy-market-reform>accessed 18 December 2018. See also Competition and Markets Authority, 'Energy Market Investigation Summary of Provisional Findings Report' (GOV.UK, 7 July 2015) available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/442500/EMI_PFs_Summary.pdf>accessed 18 December 2018.
[78] BIS (n 38) 36.
[79] Ofcom, 'Strategic Review of Consumer Switching: A Consultation on Switching Processes in the UK Communications Sector' (10 September 2010) 4.
[80] Enterprise and Regulatory Reform Act 2013, c.24.
[81] BIS (n 35) 6.
[82] ibid 6-7.

Notably, midata has a particular interest in supporting micro, small and medium-sized businesses. In response to the 2012 review, the UK Government decided to impose no midata duty on micro-businesses on the one hand, and exempt SMEs broadly from that duty on the other.[83] The Department for Business, Innovation and Skills (BIS) even considered introducing a data portability right specifically for SMEs![84] It explains that 'there is a case for extending the scope of midata to micro-businesses' to the extent that they are not only exempt from the duty to supply customer data, but can request on behalf of customers.[85] The ERRA sets as one of its primary goals 'the reform of regulatory environment faced by small and medium-sized businesses'.[86] A data portability right for the SMEs is laid down in sec 89(b), which states that a regulated person may be obliged to provide consumer data to 'a person who is authorised by a customer to receive the data at the customer's request or, if the regulations so provide, at the authorised person's request'.[87]

## IV. The Laws of Data Portability

This section provides an overview of legal regimes relating to data portability, with a focus on EU legislation. Ostensibly, the first legal regime of data portability emerged in the US at the end of the 20th century. Since then, a wide variety of schemes came into effect in the EU, pursuing various normative goals such as competition, financial innovation, consumer welfare and interoperability between public administrations. This section looks at the legacy of regimes that predate the GDPR as well as recent developments that follow.

---

[83] BIS (n 35) 7, 14.
[84] ibid 17.
[85] BIS, 'Enterprise & Regulatory Reform Bill – Midata' (BIS/13/656, February 2013) available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/86519/bis-13-656-enterprise-and-regulatory-reform-bill-midata-factsheet-feb-2013.pdf>accessed 22 December 2018.
[86] BIS, 'Enterprise and Regulatory Reform Act 2013: A Guide' (GOV.UK, 10 June 2013) 3.
[87] Enterprise and Regulatory Reform Act, 2013 c. 24, sec 89 (b).

### 1. HIPAA: Health Data Protection and Reuse

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the US Secretary of the Department of Health and Human Services (HHS) should issue privacy regulations if the US Congress fails to do so.[88] In September 2000, the HHS developed the Standards for Privacy of Individually Identifiable Health Information (known as 'Privacy Rule'), which aims to 'properly protect health information' on the one hand, and 'allow the flow of health information' on the other.[89] To implement HIPAA, the Privacy Rule introduces a right to data portability allowing the patient to[90]

- inspect information
- obtain a copy of the information
- directly transmit a copy to a designated person or entity

Pursuant to the Privacy Rule, this right to data portability is limited in many ways. It applies only to 'individually identifiable health information' in any form or media, whether it be electronic, paper or oral.[91] The right may not apply if a healthcare professional concludes that the data access is detrimental to the patient concerned or another person.[92] Interestingly, the Privacy Rule adopts a collaborative approach to determining the exchange format used. As a principle, the provision of data is, as the HHS argues, a matter of capability rather than 'willingness'.[93] The Privacy Rule prescribes that data must be provided 'in the form and format requested by the individual...if readily producible'.[94] If that is not the case, data must be provided in 'a (human) readable alternative form and format as agreed to by the covered entity and the individual'.[95] When the data concerned is retained in a digital form, the cover entity should provide it 'in a machine-readable form to the extent possible

[88] Health Insurance Portability and Accountability Act, Public Law 104–191, sec 261-4.
[89] ibid.
[90] Office for Civil Rights (OCR), 'Summary of the HIPAA Privacy Rule' (HHS.GOV, 26 July 2013) available at <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>accessed 22 December 2018.
[91] ibid.
[92] ibid.
[93] ibid.
[94] 45 CFR 164.524(c)(2).
[95] ibid.

and where consistent with the individual's request'.[96] If all options available are rejected by the requesting individual, the covered entity is allowed to provide data in a hard copy.

Building upon the success of HIPAA and MyData, the Obama Administration attempted to legislate a power that facilitates data portability in more sectors. For instance, the Consumer Privacy Bill of Rights, released in 2012, contains a consumer right 'access and correct personal data in the usable format'.[97] The administration attempted to materialise it through legislation but had not accomplished it before the General Election in 2016. The contents of this bill have ostensibly been rekindled in the recent legislative proposals, such as the CONSENT Act of 2018, [98] and Ro Khanna's Internet Bill of Rights.[99]

### 2. TFEU Art 102: The Refusal to Supply Data as an Anti-competitive Conduct

Competition law in the EU provides some remedies against undue restrictions on data flows through the market. Art 102 of the Treaty on the Functioning of the European Union prescribes that 'any abuse by undertakings of a dominant position...shall be prohibited as incompatible with the internal market'.[100] The CJEU case-law establishes that dominance in a certain market does not

[96] Health Information Privacy Division, 'Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524' (HHS.GOV, 5 February 2016) available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs>accessed 22 December 2018. See also HHS, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Non-discrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 25 January 2013, 45 CFR Parts 160 and 164.

[97] The Obama Administration, 'Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (The White House Office, February 2012) 1.

[98] Customer Online Notification for Stopping Edge-Provider Network Transgressions (CONSENT) Act, 115th Congress, 2nd session, LEW18208.

[99] Kara Swisher, 'Introducing the Internet Bill of Rights' (New York Times, 4 October 2018) available at <https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html>accessed 2 June 2019. See also Paul Bischoff, 'What is the Consumer Privacy Bill of Rights?' (CompariTech, 27 November 2018) available at <https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/>accessed 5 May 2019.

[100] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390, Art 102.

amount to a violation of competition law; only the abuse that distorts market structure should be prohibited.[101] According to the Commission's guidance, there are primarily two types of abusive conduct: [102]

- Exclusionary conduct, where a dominant undertaking excludes their competitors by other means than competing on the merits of the products or services they provide and
- Exploitative conduct, which is directly harmful to consumers through, for instance, charging excessively high prices.

Art 102 TFEU applies to the case of data portability only when an undertaking in a position of dominance *abusively* refuses to supply data to its competitors. It is operated on the premise that any refusal to supply data, an increasingly indispensable resource to compete in the market, constitutes an anti-competitive conduct. In this context, data may be considered as the essential facility, defined as 'a product or service that is objectively necessary to be able to compete efficiently'.[103] This is the case where, as the EDPS explains, 'no alternative product and service are available…and technical, legal and economic obstacles make it impossible or unreasonably difficult to develop an alternative'. [104] The doctrine of essential facility originated in the US jurisprudence, according to which owners of the essential facility are obliged to 'deal with' competitors.[105] The EU Court of Justice (CJEU) stated in *Bronner* that the refusal to supply is impermissible when an owner of an indispensable facility held more than one dominant position.[106] Beyond this point, the Court

[101] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECR 207, paragraph 189; Case T-65/89 *BPB Industries Plc and British Gypsum Ltd v Commission of the European Communities* [1993] ECR II-389, paragraph 69; Joined Cases T-24/93 to T-26/93 and T-28/93 *Compagnie maritime belge transports and Others v Commission* [1996] ECR II-1201, paragraph 107; and Case T-228/97 *Irish Sugar plc v Commission of the European Communities* ECR II-02969, paragraph 112; Case T-203/01 *Manufacture française des pneumatiques Michelin v Commission of the European Communities* [2003]ECR II-04071 paragraph 57.
[102] Richard Whish and David Bailey, *Competition Law* (7th edn, OUP 2012) 201.
[103] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and Others* [1998] ECR I-7791. Case C-418/01 *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG* [2004] ECR I-05039.
[104] 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' (Preliminary Opinion, March 2014) 21.
[105] ibid.
[106] *Bronner* (n 67) para 47.

has not explicitly recognised data as an essential facility in its judgment. That said, there exists a growing body of literature on data as essential facility, [107] and the Commission's assertion would, as Lynskey argues, be 'only a matter of time'[108]. Several scholars argue that the Court has introduced a 'forward-looking' test on whether the refusal to supply would lead to abuse of dominant position.[109] The EDPS contends that the information can be considered as an essential facility in the digital market. [110] In this market, the dominant undertakings often have 'exclusive control of the information while competitors lack the technical means to recreate the structure of system upon which the service relies'.[111] The Commission's guidance states that consumer harm is likely to arise when competitors are unable to 'bring innovative goods or services to the market' and when 'follow-on innovations are likely to be stifled'.[112] Since the competition remedy requires quite a strict threshold, it is in essence ex post and has rarely been used.

### 3. Number Portability: A Prototype for Data Portability?

Number portability does not necessarily concern the moving or exchange of data but has been seen as a source of inspiration for EU policies in relation to data portability. At the EU level, number portability is prescribed in the Universal Service Directive of 2002.[113] Recital 40 states that number portability is 'a critical facilitator of consumer choice and effective competition in a

[107] Inge Graef, *Data as Essential Facility: Competition and Innovation on Online Platforms* (Kluwer Law International 2016). Inge Graef, Damian Clifford and Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law' (2018) 8(3) International Data Privacy Law 200.
[108] Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 European Law Review 793, 799.
[109] EDPS (n 68) 21. See also Sébastien J. Evrard, 'Essential facilities in the European Union: Bronner and Beyond' (2004) 10 Columbia Journal of European Law 491.
[110] EDPS (n 68) 31.
[111] ibid.
[112] European Commission, Communication from the Commission — Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings OJ C 45, 24.2.2009, para 87. Case T-201/04 [2007] *Microsoft Corp. v Commission of the European Communities* [2007] ECR II-03601.
[113] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive), OJ L 108, 24.4.2002, p. 51–77.

competitive telecommunications environment'.[114] As per Art 30, telephone service users can retain their telephone numbers 'independently of the undertaking providing the service'.[115] This basically means that users can keep their telephone numbers unchanged when switching between service providers. Directive 2009/136/EC, which amended the Universal Service Directive, adds that the porting process should not be 'hindered by legal, technical or practical obstacles'.[116] It requires that number portability should be carried out 'within the shortest possible time' and that the loss of service during the porting process 'shall not exceed one working day'.[117]

The Directives mentioned above have been transposed into laws of every Member State. In the UK, for instance, Ofcom sets out rules about data portability, pursuant to sec 51-8 of the Communications Act of 2003.[118] The Ofcom's General Conditions of Entitlement cover both landline and mobile number portability.[119]

Obviously, number portability is distinct from the porting of data between processing systems. It remains contestable whether telephone numbers are equivalent with, for instance, consumption data about the use of telephone service. Nonetheless, number portability appears to be a major source of inspiration for policies relating to data portability in the EU. In the GDPR Impact Assessment, for instance, the practice of number portability is mentioned as a path to be followed:

*With the increasing use of certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy-friendly services become available. This could*

[114] Universal Service Directive, recital 40.
[115] Universal Service Directive, Art 30.
[116] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, OJ L 337, 18.12.2009, p. 11–36, recital 47.
[117] Directive 2009/136/EC, Art 30(4).
[118] The UK's Communications Act, 2003 c. 21, sec 51-8.
[119] Universal Service Directive, recital 40. Directive 2009/136/EC, Part C of Annex I.

*mean the loss of contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data, which is very difficult to recreate or restore. Even where possible, re-entering the data manually into another service can be a major effort. This situation effectively creates a lock-in with the specific service for the user and makes it very costly or even impossible to change provider and benefit from better services available on the market. Portability is a key factor for effective competition, as evidenced in other market sectors, e.g. number portability in the telecom sector.*[120]

## 4. The Second Payment Service Directive: Data-driven Innovation and Application Programming Interface

In the financial sector, an increasing number of data-driven technologies are transforming how consumers manage their finance. For instance, the payment initiation service (PIS) allows the consumer to make instant payment for internet bookings or online shopping without the need of a credit card.[121] Technically, the PIS makes a payment link (or software 'bridge') between accounts, automatically fill in the information for a transfer, and inform the merchant once the transaction has been initiated.[122] The Commission describes this service as 'a true alternative to credit card payments' as it allows for easy accessibility, low costs, instant payment, and immediate dispatch of goods or access to service.[123] In addition, the account information service (AIS), also known as 'account aggregation service', collects and consolidates information on several bank accounts of a consumer. In so doing, AIS gives consumers 'a global view on their financial situation'.[124] This type of service

[120] European Commission, Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, SEC(2012) 72 final, p.30.
[121] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC (PSD 2), OJ L 337, 23.12.2015, p. 35–127, Art 4(15) and recital 29.
[122] PSD2, recital 27.
[123] European Commission, 'Payment Services Directive: Frequently Asked Questions' (Factsheet, 12 January 2018) available at <http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm>accessed 21 December 2018.
[124] ibid.

also analyses spending patterns, expenses and financial needs in a user-friendly manner to help consumers make budgets and plan their finance.[125]

To facilitate innovative, data-driven services, the second Payment Service Directive (PSD2) was enacted in 2015, repealing the first Directive established in 2007.[126] Arts 66-7 of the new Directive require the Member States to ensure that users of financial services have the right to access the data in their payment accounts (if accessible online) using innovative services such as PIS and AIS.[127]

The PSD2 shall be transposed into domestic law before January 2018. In the UK, the Financial Conduct Authority (FCA) is responsible for implementing PSD2, pursuant to the Payment Service Regulation 2017.[128] According to the FCA's Policy Statement, the Open Banking Remedy is one way of making the PSD2 requirements possible.[129] Similarly, the CMA states that, with open banking, there is no need for banks to 'put in place other measures to comply with the PSD2'.[130]

The idea behind Open Banking was first expressed in the ODI/Fingleton Report, which looks at how banking data can be reused through API and Open Data.[131] The Open Banking Working Group was established in 2015 and published the standards for open API in the following year.[132] In August 2016,

[125] ibid.
[126] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC (PSD 2), OJ L 337, 23.12.2015, p. 35–127.
[127] PSD2, Arts 66-7.
[128] The UK's Payment Services Regulations, 2017 No. 752.
[129] Financial Conduct Authority, 'Implementation of the Revised Payment Services Directive (PSD2): Approach Document and Final Handbook Changes' (Policy Statement PS17/19, September 2017) 5.
[130] CMA, 'Retail Banking Market Investigation: Provisional Decision on Remedies' (GOV.UK, 17 May 2016) 48.
[131] Open Data Institute and Fingleton Associates, 'Data Sharing and Open Data for Banks: A Report for HM Treasury and Cabinet Office' (HM Treasury, September 2014) 5.
[132] Open Banking Working Group, 'The Open Banking Standard: Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation' (Open Data

the CMA released the results of its investigation into UK's retail banking market, which suggested several remedies including Open Banking.[133] According to the CMA's report, Open Banking means that the largest retail banks in the UK (as well as a few challenger banks) should develop and adopt an open API banking standard by January 2018.[134] Open API would allow consumers to use innovative services and monitor their usage in a real-time manner. The analysis of their spending would also 'harness insights to identify better deals and automatically switch to them'.[135] To deliver this remedy, the Open Banking Implementation Entity (OBIE) was set up in 2016.[136]

The UK Government takes Open Banking as a testbed for data-based innovation. As the BIS puts it, 'open banking is a revolutionary move in this direction...and we want to understand how this approach can be successfully implemented in other regulated sectors'.[137] To this end, it called for a 'Smart Data Review' in 2018 to consider how data portability accelerates the development and use of data-driven technologies.[138]

### 5. Free Flow of Non-Personal Data and Supply of Digital Content: Combating Lock-in

In May 2015, The Commission released the Digital Single Market Strategy to facilitate data flows in the EU further, among 15 other objectives.[139] Two years later, the Commission tabled a proposal for a Regulation dealing with the

---

Institute, 8 February 2016) available at <https://www.scribd.com/doc/298569302/The-Open-Banking-Standard>accessed 21 December 2018.

[133] CMA, 'Retail Banking Market Investigation: Final Report' (GOV.UK, 9 August 2016) xxxviii.

[134] CMA (n 94) 48.

[135] BIS, 'Modernising Consumer Markets: Consumer Green Paper' (GOV.UK, 11 April 2018) 23.

[136] Open Banking, available at<https://www.openbanking.org.uk>accessed 21 December 2018.

[137] ibid 22.

[138] Department for Digital, Culture, Media and Sport and Department for Business, Energy & Industrial Strategy, 'Policy Paper: Smart Data Review' (GOV.UK, 28 September 2018) available at <https://www.gov.uk/government/publications/smart-data-review>accessed 21 December 2018.

[139] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, 06.05.2015, COM(2015) 192 final.

barriers to the free flow of non-personal data (FFNPD).[140] This Regulation rapidly came into effect in 2018, one year before its introduction.[141] The FFNPD framework, which applies only to data other than personal data, was introduced as a supplement to the GDPR.[142] The Commission notes that while there exists a right to data portability in the GDPR for natural persons (data subject), the ability to port data and to switch service providers is not guaranteed for professional users, those who use data processing services for trade, business, craft, profession or task.[143]

In the consumer market, the Digital Content Directive (DCD) was recently approved in April 2019, which allows the consumer (those acting for purposes outside his or her trade, business, craft, or profession) to retrieve non-personal data upon termination of the contract.[144] While the Commission initially proposed to create a portability scheme parallel to the GDPR[145], the Digital Content Directive is eventually devised as a supplement as well. In this new landscape, the GDPR allows for the porting of personal data, whereas the Directive further supports that of non-personal data relating to the supply of digital content or the use of digital service. The issue of how these new instruments interplay with the GDPR will be detailed in Chapter 3.

### 6. European Interoperability Framework: Lessons from the Public Sector

To achieve the interoperability between public administrations, the EU has developed a set of standards, principles and specification in the public sector.

---

[140] European Commission, Proposal for a Regulation of the European Parliament and of the Council on A Framework for the Free Flow of Non-personal Data in the European Union, COM(2017) 495 final.
[141] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (FFNPD), OJ L 303, 28.11.2018, p. 59–68.
[142] Regulation 2018/1807, Art 3(1).
[143] Regulation 2018/1807, recital 29 and Art 3(8).
[144] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services (Digital Content Directive), OJ L 136, 22.5.2019, p. 1–27, Art 16(4).
[145] European Commission, 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) 634 final.

The interoperability policy at the EU level can be traced back to the 1990s when the Commission decided to build trans-European networks for data exchanges between public administrations.[146] In 2010, the Commission established the European Interoperability Framework (EIF) through its Communication titled 'Towards Interoperability for European Public Services'.[147] Principally, the EIF provides guidance to public administration on interoperability activities and ensures that new legislation does not compromise interoperability efforts.[148] Pursuant to the Digital Single Market Strategy[149], the Commission called for the extension of the EIF in 2015 and, in the same year, the ISA² programme was established to maintain and develop that framework.[150] In 2017, the Commission updated the EIF with a set of 12 underlying principles, notably including data portability, reusability, technology neutrality, user-centricity, among others.[151] The Commission states that the functioning of the digital single market 'requires data to be easily transferable among different systems to avoid lock-in, and support the free movement of data'.[152] Notably, a layered model of interoperability is also recommended in this framework, which, as will be shown in Chapter 5, would ease the understanding of related legal requirements concerned data portability and interoperability.

[146] 1719/1999/EC: Decision of the European Parliament and of the Council of 12 July 1999 on a Series of Guidelines, including the Identification of Projects of Common Interest, for Trans-European Networks for the Electronic Interchange of Data between Administrations (IDA) OJ L 203, 3.8.1999, p. 1–8.
[147] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Towards Interoperability for European Public Services, 16.12.2010, COM(2010) 744 final.
[148] European Commission, *New European Interoperability Framework: Promoting Seamless Service and Data Flows for European Public Administrations* (Publications Office of the European Union, 2017) 4.
[149] European Commission (n 110) 15.
[150] Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, Establishing a Programme on Interoperability Solutions and Common Frameworks for European Public Administrations, Businesses and Citizens (ISA² programme) as a Means of Modernising the Public Sector, OJ L 318, 4.12.2015, p. 1–16.
[151] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework – Implementation Strategy, COM(2017) 134 final.
[152] European Commission (n 104) 15.

# V. Observations and Conclusion

This chapter aims to foster a fuller understanding of data portability and its normative values. It shows a broad spectrum of data portability schemes, whether they be industry-initiated projects, government-led initiatives or legal regimes (shown in the table below).

| Scheme | Established since | Type | Sector | Data concerned | Purpose |
|---|---|---|---|---|---|
| HIPAA/Privacy Rule | December 2000 | Legal regime | Healthcare | Medical data | Health data protection and data flow |
| Number Portability | April 2002 | Legal regime | Telecommunication | Telephone numbers | Consumer choice and effective competition |
| Blue Button (MyData) | January 2010 | Government-led | Health | Health data | Improve healthcare and health data control |
| midata | April 2011 | Government-led | Energy, Telecom, and Banking | Transaction and consumption data | Competition and consumer empowerment |
| Google Takeout | June 2011 | Industry-initiated | Digital | User data | 'Liberating' Google products |
| Green Button (MyData) | 2012 | Government-led | Energy | Usage data | Energy use management and environmental protection |
| MyStudentData (MyData) | 2012 | Government-led | Education | Student personal data | Informed decision-making by the students |
| Evernote | June 2014 | Industry-initiated | Digital | User data | User trust |
| Data Transfer Project | 2017 | Industry-initiated | Digital | User data | Open ecosystem |

| | | | | | |
|---|---|---|---|---|---|
| Payment Service Directive II | January 2018 | Legal regime | Financial | Bank data | Data-driven innovation |
| Open Banking | January 2018 | Government-led | Financial | Transactional data | Data-driven innovation and competition |
| General Data Protection Regulation | May 2018 | Legal regime | All | Personal data | Personal data protection and data flows |
| Free Flow of Non-Personal Data | November 2018 | Legal regime | All | Non-personal data | Competitive data economy |
| Digital Content Directive | April 2019 | Legal regime | Digital | Non-personal data | Consumer choice and effective competition |

Table 1.1 Data portability schemes examined in chronological order (including the General Data Protection Regulation of 2016)

The survey of existing schemes shows that the meaning of data portability, as well as the methods of delivery, has evolved over time. For a long time, data portability had been associated with the objective of switching (*data portability for switching*) and, in this context, data plays an informative role in bringing knowledge and insights to consumers. When a telephone service contract is up for renewal, for instance, a subscriber may request his or her billing history and compare it with alternative offers in the market. Empirical research shows that consumers do not often switch because they lack knowledge about their consumption or usage.[153] The construction of that knowledge, however, depends upon whether the useful information is readily accessible on the one hand, and whether the consumer has the capacity to understand or process that information on the other. Not all data is readily straightforward to an average individual; some technical, complex datasets do not make any sense unless further processed. In the case where data is not reasonably understandable by humans, data portability schemes demand that data should

[153] BIS (n 38) 49.

be at least machine-processable to deliver human-comprehensive results. Green Button, for instance, requires that energy usage information be provided in a 'consumer-friendly and computer-friendly format'.[154] midata encourages the transaction data to be released 'in a reusable, machine-readable form and in an open standard format'.[155] The CASG promises consumers that they can download their banking data in a 'Common Separate Value' (CSV) file and upload it for gaining insights.[156] As will be shown later, these format requirements have been well reflected in the EU legal rules concerning data portability.

In the digital age, data processing now becomes a distinct type of service, *i.e.* data as a service (DaaS), and many sectors, even including those brick-and-mortar ones, have prepared themselves to provide data-driven services. In such a datafied society, the need for data portability has also increased, and the methods of delivery diversified. Web2.0 now enables internet users to generate a large amount of data concerning their identities, intellectual creations and everyday lives. When the market provides new options that are potentially better, cheaper and privacy-friendly, these users could consider switching or changing the preference of data processing. For businesses, the tasks of collating, storing and managing databases can now be outsourced to cloud specialists.[157] It is noted that businesses have the incentive to migrate data from in-house premises to the cloud or between clouds. In these cases, the porting of data itself equates with the switching of service (*data portability as switching*).

---

[154] Energy.Gov (n 26). See also Aneesh Chopra, 'Modelling a Green Energy Challenge after a Blue Button' (White House Archive, 15 September 2011) available at <https://obamawhitehouse.archives.gov/blog/2011/09/15/modeling-green-energy-challenge-after-blue-button> accessed 17 December 2018.
[155] BIS, 'midata: 2012 Review and Consultation' (GOV.UK, 27 July 2012) 23.
[156] HM Treasury and The Rt Hon George Osborne, 'Bank Account Switching Service Set to Launch' (GOV.UK, 10 September 2013) available at <https://www.gov.uk/government/news/bank-account-switching-service-set-to-launch>accessed 22 December 2018.
[157] Robert Carpenter, 'Walking from Cloud to Cloud: The Portability Issue in Cloud Computing' 6(1) Washington Journal of Law, Technology & Arts 1, 1.

The emergence of API prompts us to rethink data portability, and in particular, its historical link with switching. Should an automatic exchange of data be made available, one does not have to physically port data out of a system to reuse it in a new environment (*data interoperability without the need for switching*). As will be argued in the next chapters, the API-based exchange does not remove the need for data portability. When popular services intrusively abuse user data or cease to provide services, as frequently shown in reality, users do intend to leave a certain service with their data.[158]

Apart from the evolving nature of data portability, this chapter reveals the trajectory of policy- and law-making concerning data portability, with a focus on EU and UK. It is shown that early schemes that predate the GDPR are limited in several ways: these schemes narrowly apply to selected sectors, and the types of data concerned are plain information (or numbers). More recent schemes, such as legislations at the EU level, have broadened the scope of application and the scope of data concerned. In brief, the GDPR seems to have duly incorporated the legacy of early developments. As will be shown in the next chapter, this new Regulation represents a holistic approach to personal data flows and distinctively frames data portability as a means of data protection.[159] The new right to data portability is ostensibly applicable to all sectors but inherently associated with the objective of data protection. With the potential to promote other objectives such as consumer welfare, the GDPR right needs to be used in tandem with other regimes. Given the GDPR's

[158] Anthony Cuthbertson, 'Google+ to Shut down Early after Data from 52 Million Users Exposed' (Independent, 11 December 2018) available at <https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-plus-shut-down-date-bug-personal-data-breach-alphabet-inc-a8677296.html>accessed 20 December 2018. Kaitlyn Tiffany, 'Angry Birds and the End of Privacy' (Vox, 14 May 2019) available at <https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush>accessed 3 June 2019.

[159] The GDPR right is generally inapplicable to the public sector due to its scope of application. As per Art 20(1), the right applies to data processing based on consent or contract but data controllers in the public sector often have alternative bases for data processing, such as legal obligation (art 6(1)(c)) or public interest (art 6(1)(e)). This application issue was raised in many DAPIX meetings, and the representatives concluded that there was no need to make more explicit the right's inapplicability to the public sector in recognition of the right's limited scope. In addition, my unsuccessful request of data portability to the UK Border Agency on 25 May 2018 also provides an illustration of this.

limitations in scope, recent EU instruments are devised, as the supplements to the GDPR, to facilitate the flow of data more broadly. In this evolving landscape, the GDPR now facilitates the porting of personal data while both the FFNPD and the DCD the promote that of non-personal data. The following chapters will give a detailed analysis of how this GDPR right differs from existing schemes and interplays with the new ones.

At a time when the EU is keen on legislating on data portability, it should be noted that the pre-existing schemes are evolving at the same time. For instance, midata was initially considered as 'a very narrow use case about trying to shop around for the best current account'.[160] Since 2015, however, the BIS is exploring new ways to address the frictions in the switching process, in addition to midata. The results of a 2015 public consultation on switching principles show that there is 'less evidence consumers can easily use data to authorise third parties'.[161] As BIS puts it, while midata is 'a crucial step to address one of the biggest frictions in the switching process', new methods such as Application Programming Interface would 'make the process even more streamlined and accessible'.[162] In the Green Paper on Modernising Consumer Markets, the BIS advocates the automated approach to data portability, which would allow consumers to 'benefit from new technology and new business models'.[163] Similarly, in the US, the Obama administration was committed to 'pushing data on the internet in machine-readable formats to advance the goals of innovation, transparency, participation and collaboration'.[164] To implement Green Button, the Smart Grid Interoperability Panel built an 'Energy Service Provider Interface' (ESPI), allowing for automatic transfer of energy data to third parties. Once connected, innovative services can 'programme home energy management service, sizing and

[160] ibid.
[161] BIS, 'Switching Principles: Government Response and Action Plan' (GOV.UK, May 2016) 33.
[162] ibid 33.
[163] BIS (n 99) 7.
[164] Obama Administration (n 61) 20.

financing rooftop solar panels, and helping a contractor to verify their savings more effectively'.[165]

In sum, data portability has been sought for several goals such as competition, consumer welfare, innovation and institutional efficiency. Most schemes examined above have due consideration of data privacy, security and data protection but are not designed to protect our personal data. The next chapter provides a detailed account of data portability as a new way to protect our personal data.

[165] ibid.

# Chapter 2 Examining the Right to Data Portability through the Lens of Data Protection: Legitimacy, Consistency and Added Value

## Introduction

The previous chapter illustrated with ample examples that individuals, industries and governments have sought data portability for varied reasons. It has a contested impact on competition, facilitating the growth of an emerging industry specialising in user-centric technological systems. Data portability may also facilitate consumer welfare by freeing consumers from lock-in and allowing them to enjoy better, cheaper and more privacy-friendly services in the market, if any. With user-side technologies, consumers can even extract added value from their personal data for themselves. The data-driven innovation and institutional efficiency that data portability facilitates also benefit individuals in many ways.

Despite these tangible values, data portability has recently been associated with the goal of data protection in the EU legal order and more. This marriage seems anti-intuitive at the outset because the act of moving data out of a secured system instantly invites threats to data privacy, security and integrity.[1] Nevertheless, the GDPR brings in data portability to enhance individual control over personal data further.[2] The underlying rationale is that data portability represents a new opportunity for personal data flows from systems exclusively controlled by organisations to those centred on users. With the advent of user-centric technological systems, our personal data may be better protected by

[1] Andrew Cormack, 'Portability Right: A Data Protection Challenge' (JISC Community, 19 April 2017) available at <https://community.jisc.ac.uk/blogs/regulatory-developments/article/portability-right-data-protection-challenge>accessed 25 May 2019.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) OJ L 119, 4.5.2016, recital 7.

moving them away from the 'surveillance capitalism'.[3] That said, the right-based data portability begs the question as to how data portability interfaces with data protection law, including its objectives and instruments. This chapter explores whether and to what extent the new right to data portability sits legitimately and coherently within the EU data protection framework.

The structure of this chapter is as follows. It first ventures to justify the new GDPR right on the basis of the free movement of personal data. To deal with this issue, it looks at the complex relationship between data protection and data mobility in this framework, as well as the constitutional changes brought by the Lisbon Treaty. Second, this chapter provides a brief historical overview of the GDPR and its new right to data portability. Since the right is devised to facilitate the goal of enhancing individual control over personal data, the chapter traces back to this goal's ostensible origin in German constitutional jurisdiction. It looks at how the right to informational self-determination sheds light on the evolution of data protection and data portability in Germany and beyond. Despite the legitimacy issue, this chapter also looks at how the new right interacts with the existing rights, such as the right of access and the right to erasure. It is argued that the right to data portability should be clearly differentiated from the right of access, and be appropriately balanced with the right to erasure. Further, strategies should be provided to the data subject to jointly and holistically use these rights. Last, it is worth exploring the right's interplay with the new principle of data protection by design and by default. It will be revealed that some technical measures encouraged by this principle would impede the enforcement of the GDPR rights.

## I. Data Portability and the Free Flow of Personal Data

As argued earlier, the new right to data portability is fundamentally distinct from conventional components of EU data protection law. From the outset, it keeps a tenuous link to data protection but appears much closer to the objective of the free flow of personal data. This section first provides a historical overview

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

of this economic objective, followed by an analysis of its relation to the objective of data protection in the EU data protection regime. Last, the section examines whether the free flow of personal data may lend normative support, by itself, to schemes such as the right to data portability.

## 1. Free Flow of Personal Data: A Historical Trajectory

Initially, the rationale of the free flow of personal data derived from the imperative to establish an internal market in the EU. Art 8a of the Treaty establishing the European Community (TEC) states that the Community shall adopt measures to establish the internal market progressively. The Data Protection Directive was established upon Art 100(a) (now Article 114 TFEU[4]), which requires that an internal market be established through approximating the law, regulation and administrative action in Member States.[5] After the Lisbon Treaty, the EU acquired the competence to legislate on data protection, with Art 16 recognising a right to data protection for everyone and providing an independent basis for EU secondary law.[6] It requires the EU legislative bodies to lay down the rules relating to data protection and the free movement of such data.[7]

Three attributes of the goal of the free flow of personal data are observed below. First, the free flow of personal data is customarily referred to in a transboundary context. Also known as the free movement of personal data in the Union, this objective is an integral part of the internal market in the EU. As the Commission states, the free movement of goods, persons, services and, capital (*i.e.* the four fundamental freedoms) demands that personal data is transferable between businesses involved in cross-border activities.[8]

---

[4] Consolidated Version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, Art 286.
[5] Treaty Establishing the European Community (Consolidated version 2002) OJ C 325, 24.12.2002, p. 33–184, Art 100(a).
[6] TFEU, Art 16(1).
[7] TFEU, Art 16(2).
[8] Commission of the European Communities, Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security COM(90) 314 final, 16.

Second, as individuals were incapable of directing data flows when the Data Protection Directive was enacted, the free movement of personal data had not been materialised at the individual level. In the Communication on data protection and information security, the Commission states that cross-border data flows were 'apparent at three levels':

1. Between businesses: personal data is used at numerous stages of economic activity
2. Cooperation between national authorities: the flow of data is essential to the Community integration process and in particular the abolition of frontiers
3. Scientific cooperation purposes

While the Commission states that it 'respects the rights of data subjects', the Data Protection Directive did not entail a right to data portability.[9] The free flow of personal data was mainly a catalyst of the internal market, and hence the data flows between businesses and consumers were not mentioned at all.

Third, as the free flow of personal data was primarily achieved through harmonisation of domestic law, there existed no specific regime directly facilitating this economic objective. In this respect, Lynskey argues that the EU had 'no legal mechanism or Treaty basis to remove obstacles on an *ad hoc* basis'.[10] As a result, the EU had to ensure personal data flow 'via positive integration by creating a harmonised legal environment'.[11] Indeed, both the Directive[12] and the Regulation[13] identify the fragmented implementation of the Directive as the major obstacle to data flows. To remove it, the GDPR ensures 'consistent and homogenous application' of data protection rules and hence equivalent protection in all Member States.[14]

---

[9] ibid.
[10] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 49-50.
[11] ibid.
[12] 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 OJ L 281, 23.11.1995, recital 7.
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) OJ L 119, 4.5.2016, recital 9.
[14] GDPR, recital 10.

The facts that all components of the data protection Directive were contributing solely to data protection, and that the economic objective achieved as a result ostensibly implies a sequence of achievement: should the protection of personal data be consistently ensured among the EU Member States first, the flow of personal data can then be guaranteed.

Further to personal data flows, the EU recently has legislated on the free movement of data other than personal data. In its Communication, the Commission expresses the concern about the legal vacuum left by the data protection regime: while the GDPR facilitates personal data flows on the ground of data protection, there is a growing need to promote data flows more widely in order to contribute to a 'competitive data economy'.[15] Consequently, the Digital Single Market Strategy aims to 'remove and prevent any unnecessary restrictions regarding the location of data within the EU'.[16] As part of this strategy, a framework of the Free Flow of Non-Personal Data (FFNPD) was proposed in 2017.[17]

Arguably ruling out the concerns of data protection, this Regulation has been rapidly approved within a year since its inception.[18] Art 1 states that this Regulation ensures 'free movement of data other than personal data' by restricting data localisation requirements. Apart from transborder data flows,

[15] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303, 28.11.2018, p. 59–68, Art 6(1).
See also European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards A Thriving Data-driven Economy COM(2014) 442 final. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building A European Data Economy" COM(2017) 9 final.
[16] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe COM(2015) 192 final, p.15.
[17] Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union COM (2017) 495 final
[18] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal data in the European Union (FFNPD), OJ L 303, 28.11.2018, p. 59–68.

this Regulation also encourages the porting of data across technical systems. Recital 29 of the Regulation explains that whereas individuals benefit from the GDPR, the ability to switch between services providers or port data to other systems is not facilitated for professional users, those who act in the course of their business or professional activities.[19]

## 2. The Interplay between Data Protection and Data Mobility

In general, EU data protection regime pursues two goals at the same time: it protects natural persons in relation to the processing of personal data and ensures free movement of personal data in the European Union.[20]

Before the Lisbon Treaty, the economic rationale was in fact of greater significance. As the EU did not have the competence to legislate on human rights, the economic rationale was the primary and arguably the only legitimate basis for this Data Protection Directive. For instance, Advocate General Tizzano states in *Lindqvist* that Art 100a TEC was not a basis for 'measures that were not justified by the objective of encouraging the establishment and functioning of the internal market'.[21] Should the protection of fundamental rights (in particular the right to privacy) be considered as 'the other, independent objective...the very validity of the Directive might be called into question'.[22] This reasoning is, however, outdated after the TFEU introduced an independent legal basis for data protection. Consequently, the EU data protection law now does not have to rely on the market integration rationale and has obtained additional support from Art 8 of the EU Charter of Fundamental Rights (CFR).[23] Lynskey notes that the CJEU 'initially emphasised the market integration objective...with its fundamental rights

[19] Regulation (EU) 2018/1807, Art 3(8).
[20] 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, OJ L 281, 23.11.1995, Art 1.
[21] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, Opinion of Mr. Advocate General Tizzano delivered on 19 September 2002, para 42.
[22] ibid.
[23] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407, Art 8.

objective playing a merely secondary role'.[24] The Lisbon treaty has, however, 'loosened the link between data protection legislation and the internal market' and placed the two objectives on an equal footing. Several issues arise in the wake of this paradigmatic change: if the two objectives are of equal normative weight, can either of them now independently provide normative support for a specific scheme, such as the right to data portability? More specifically, should the free flow of personal data always be associated with data protection to lend support to the right to data portability? These issues will be addressed in the following.

## 3. Free Flow of Personal Data as an (Independent) Legal Basis?

While all specific schemes in the Data Protection Directive contribute solely to the goal of data protection, the new right to data portability in the GDPR appears to be an exception. This right is more naturally associated with the objective of the free flow of personal data, by facilitating data flows *across systems* and, intermittently, transborder data flows. As businesses distribute their IT facilities globally, the processing systems concerned may be located within different Member States.

Nevertheless, there are two main aspects where the data portability right does not fit fully the objective of the free movement of personal data. First, the right is concerned with data flows *across systems* while the free flow of personal data has been interpreted in a *transboundary* context. While the participating systems may locate in different countries, the flows of data directed by individuals would not always cross boundaries. Second, the free movement of personal data is ensured by preventing Member States from imposing restrictions grounded on data protection. In contrast, the implementation of Art 20 GDPR is primarily at the individual level and depends much on the data controller's accountability.

[24] Lynskey (n 7) 47.

In due recognition of the linkage between the right and the objective, it is argued that free movement of personal data should at least partially lend support to the data portability right, together with the objective of data protection. These two objectives are interdependent values, inherently associated with each other in the EU data protection framework. On the one hand, the promotion of data flows is strictly associated with data protection rules. On the other, the consistent application of data protection rules has a desired impact on the data economy. Therefore, the economic objective should not independently lend support to the data portability right, without resort to the objective of data protection.

This observation has recently been reinforced by the divide between flows of personal data and those of non-personal data. In the FFNPD framework, the porting of data is a critical way of facilitating data flows. The pursuit of data portability in this context implies a strong link between transborder data flows and cross-system data portability. More importantly, the Regulation seems to suggest that only the processing of non-personal data can be decoupled from the rationale of data protection. This would indirectly reassure the intrinsic link between data protection and data flow in the EU data protection regime.

That said, this thesis proposes a radical proposition about the two objectives and the sequence of achievement in particular. Conventionally, data protection rules should first be consistently implemented so that the free flow of personal data between Member States can be ensured. In the case of data portability, however, these two objectives might be achieved in reverse order. By facilitating flows of personal data across systems and, intermittently, across borders, this right would foster a data protection culture in the long run. The demand for better systems in terms of security, control, transparency, openness, interoperability, and accountability will increase when individuals proactively port, manage and protect their data.[25] Incumbent and new service

[25] For instance, see Jason Furman and others, 'Unlocking Digital Competition: Report of the Digital Competition Expert Panel' (Digital Competition Expert Panel, March 2019).

providers would be incentivised to develop those systems to meet that demand. Eventually, the increased flow of data by individuals would produce a positive impact on data protection. In this broad sense, the right to data portability can be seen as pursuing both data protection objectives, albeit in an unconventional manner.

## I. GDPR and Data Portability: A Historical Overview

The Directive 95/46/EC had weathered almost two decades of technological and legal changes before replaced by the new General Data Protection Regulation (GDPR) in May 2018.[26] In early 2012, the European Commission put on the political agenda a proposal for a new GDPR.[27] The Impact Assessment states that while the objectives and principles of the Directive remained sound, it had not prevented 'fragmentation in the way data protection is implemented across the Union'.[28] The proposed GDPR represented a stronger and coherent framework that will 'put individuals in control of their own data' on the one hand and 'reinforce legal and practical certainty for economic operators' on the other.[29]

Between the Directive and the Regulation, there had been significant changes in the EU legal order. The Lisbon Treaty introduced an independent legal basis for data protection so that secondary law in this field does not have to rely upon

[26] 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 OJ L 281, 23.11.1995, p. 31–50.
[27] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 25.1.2012, COM(2012) 11 final.
[28] European Commission, Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, 25.1.2012, SEC(2012) 72 final, p. 7.
[29] ibid 8.

the market integration rationale.[30] Further, the new EU Charter of Fundamental Rights, which entered into force in 2009, introduced a new fundamental right to data protection.[31] The GDPR, now built upon Art 16 of the Lisbon Treaty and Art 8 of the EU Charter, well reflects these constitutional changes. After roughly four years of deliberation, the final version of this Regulation was approved in May 2016 and became effective on 25 May 2018.[32]

This new piece of EU legislation has a number of innovations. Among others, it is known for the strengthening of subject rights and, correspondingly, provides for enhanced accountability and heavier responsibilities for data controllers.[33] All subject rights in Art 12 of the Directive have been expanded and clarified in several Articles of the GDPR.[34] To note, the right to be forgotten has been framed as a new right of the GDPR. However, it can find its roots in Art 12 of the Directive,[35] and has been developed in the CJEU jurisprudence well before the GDPR comes into effect.[36] Apart from the subject rights, the GDPR emphasises the significance of design for data protection. Ostensibly inspired by the recent conceptual development of Privacy by Design (PbD)[37], it lays down the principle of Data Protection by Design and by Default in Art 25, requiring the data controllers to take measures to implement the data protection principles and safeguard the subject rights.[38]

---

[30] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 OJ C 306, 17.12.2007, p. 1–271, Art 16.
[31] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, Arts 7-8.
[32] Regulation (EU) 2016/679 (n 2).
[33] GDPR, Arts 5(2), 24 and 32.
[34] GDPR, Arts 15-22.
[35] Data Protection Directive, Arts 12, 14, 15.
[36] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317. See also Case C 398/15 *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce versus Salvatore Manni* ECLI:EU:C:2017:197.
[37] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles', available at <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>accessed 22 May 2019. See also Ann Cavoukian, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices' (2010) 3(2) Identity in the Information Society 405.
[38] GDPR, Art 25.

This thesis mainly looks at the right to data portability laid down in Art 20,[39] as well as its interaction with other components of EU data protection law, old and new. Within four years of legislation, the framing of the right to data portability was in huge controversy. As will be shown throughout the thesis, the objectives, conditions, and specifications of this have been drastically altered. The final text of Art 20 GDPR, which is much more comprehensive than the original[40], is as follows:

> Article 20 Right to data portability
>
> 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.

[39] GDPR, Art 20 and recital 68.
[40] For comparison, Art 18 of the proposal by the Commission states as follows:

Article 18 Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

> 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
>
> 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

The creation of such a right for data subjects was unprecedented in the EU. As Commission puts it, there existed no explicit right in the Directive to 'extract his/her own personal data from an application or service in a format that may be processed further, so that the individual may transfer data to another application or service'.[41]

There is also no comparable legal regimes elsewhere in the world except the US Health Insurance Portability and Accountability Act of 1996 (HIPAA).[42] Pursuant to his Act, a right to access medical records narrowly applies to the medical sector.[43] To note, the Philippine Data Privacy Act of 2012 introduced a right to data portability that entered into force earlier than its GDPR counterpart. However, this right under the Philippine legislation substantially mirrors Art 18 of the GDPR proposal and, due to its early adoption, has not accommodated the subsequent changes made by the EU legislative bodies after then.

The creation of the right to data portability in the GDPR has influenced the development of data protection in other jurisdictions. For instance, the Digital Republic Act (*Loi n°2016-1321 pour une République numérique*) was passed in France, shortly after the EU approved the GDPR in 2016. As the 'first national implementation of the GDPR right to data portability', this Act introduced a more extended right than Art 20 GDPR. The French right applies

[41] European Commission (n 5) 30.
[42] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
[43] Office for Civil Rights (OCR), 'Summary of the HIPAA Privacy Rule' (HHS.GOV, 26 July 2013) available at <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>accessed 22 December 2018.

to personal data as well as 'other data facilitating the switch from one service to another'.[44]

In Latin America, Argentina released its modernised data protection bill in 2017, to replace the Argentine Data Protection Law of 2010.[45] This Act is known for being heavily based on the GDPR and for introducing a data portability right for the first time in Argentine legal order.[46] Brazil approved its new General Data Protection Law in August 2018, in which a right to data portability is created as part of the right of access.[47] Notably, this new law acknowledges as the basis for data protection both the ownership of personal data by all natural persons and informational self-determination.[48]

In the US, the Obama Administration introduced a 'Consumer Privacy Bill of Rights' in 2012, according to which a consumer has the right to 'access and correct personal data in usable format'.[49] This administration intended to materialise the Bill of Rights through Federal legislation, but this attempt appears to have failed to do so after the General Election in 2016.[50] In the wake of the Cambridge Analytica scandal[51], the Californian Consumer Privacy

[44] Dessislava Savova and others, 'French Law for A Digital Republic Anticipating the Impact of the GDPR' (Talking Tech, 17 April 2017) available at <https://talkingtech.cliffordchance.com/en/data-cyber/data/french-law-for-a-digital-republic-.html>accessed 19 February 2019.
[45] Hunton Andrews Kurth, 'DPA of Argentina Issues Draft Data Protection Bill' (Privacy & Information Security Law Blog, 9 February 2017) available at <https://www.huntonprivacyblog.com/2017/02/09/dpa-argentina-issues-draft-data-protection-bill>accessed 19 February 2019.
[46] ibid.
[47] Renato Leite Monteiro, 'The New Brazilian General Data Protection Law — A Detailed Analysis' (iAPP, 15 August 2018) available at <https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>accessed 4 May 2019. Brazilian General Data Protection Law, Arts 18-9. See also the English Version of Brazilian General Data Protection Law (Ronaldo Lemos and others trs), available at <https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf>accessed 4 May 2019.
[48] Brazilian General Data Protection Law, Arts 2 and 17.
[49] The Obama Administration, 'Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (The White House Office, February 2012) 1.
[50] Paul Bischoff, 'What is the Consumer Privacy Bill of Rights?' (CompariTech, 27 November 2018) available at <https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/>accessed 5 May 2019.
[51] The California Consumer Privacy Act of 2018 (CCPA), AB-375.

Act (CCPA) was signed into law in June 2018. This Act also incorporates a 'right to data portability', allowing consumers to obtain personal information in a 'portable and to some extent technically feasible, in a readily usable format'.[52] Notably, the CCPA allows a Californian consumer to make two requests only every year.[53] More recently, US Representative Ro Khanna proposed to extend the Californian Act to other states in the US through the Internet Bill of Rights.[54]

Discussions about introducing a new right to data portability are also undergoing elsewhere in the world. The OECD report reveals that both Japan and Australia are possibly writing data portability right into domestic law.[55] Greenleaf notes that the data portability right, as a 'third-generation principle', has informed the development of data protection in jurisdictions outside the EU.[56] After the GDPR was approved in 2016, the Council of Europe initiated a process of modernising the Convention 108 through the Protocol CETS No.233.[57] While the process is, as Greenleaf puts it, 'GDPR lite', a few innovations such as the right to data portability, are not reflected in the modernised text.[58]

[52] CCPA, 1798.100(d).
[53] ibid.
[54] Ro Khanna, 'Internet Bill of Rights', available at <https://www.rokhanna.com/issues/internet-bill-rights>10 May 2019.
[55] OECD, 'Expert Workshop on Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use' (SPDE(2018)4, 19 April 2018) para 32.
[56] Graham Greenleaf, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' (2017) 145 Privacy Laws & Business International Report 10.
[57] Council of Europe, 'Convention 108 and Protocols', available at <https://www.coe.int/en/web/data-protection/convention108-and-protocol>accessed 17 February 2019.
[58] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final. See also Graham Greenleaf, 'Renewing Convention 108: The CoE's "GDPR Lite" Initiatives' (2016) 142 Privacy Laws & Business International Report 14.

## II. Individual Control and Informational Self-determination: Towards a Justification for the Right to Data Portability

The nature of the GDPR right to data portability appears fluid in legislative drafts and guidelines,[59] and is highly contested in scholarly literature.[60] In the final version of the GDPR, this right has as its only objective the strengthening of individual control over personal data.[61] The Article 29 Working Party explains that enhanced control allows the data subject to 'play an active role in the data ecosystem'.[62] In the GDPR impact assessment, the Commission also aligns the goal of enhanced control with consumer trust in the online environment, alluding to the right's desirable impact on e-commerce.[63]

Scholarly efforts have been made to link the EU notion of control with the concept of informational self-determination to justify the new GDPR right on that basis. For instance, Purtova argues that the right to data portability can be seen as 'a logical extension to the notion of informational self-determination'.[64]

---

[59] For instance, the Commission stated that the right to data portability is devised to ensure that 'individuals are in control of their personal data and trust the digital environment'. In an earlier draft, the European Parliament sees the right as a strengthening of the right of access. The Article 29 Working Party once claimed that data portability is to 'facilitate switching...thus enhance competition between services'. See European Commission (n 5) 43. Jan Philipp Albrecht, Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), A7-0402/2013, 21.11.2013, recital 55. Article 29 Working Party, 'Guidelines on the Right to Data Portability' (WP242, 13 December 2016) 4.

[60] Gabriela Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 2(3) International Data Privacy Law 149. Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) Maryland Law Review 335. Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42(6) European Law Review 793. Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22(2) Personal and Ubiquitous Computing 317. Helena Uršič, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15(1) SCRIPTed 42. Paul Quinn, 'Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?' (2018) 18(2) Global Jurist 81.

[61] GDPR, recital 68.

[62] Article 29 Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 4.

[63] European Commission (n 5) 43.

[64] Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-determination Off the Table, and Back on Again?' (2014) 30(1) Computer Law & Security Review 6, 15.

Similarly, Custers and Uršič contend that data portability, from an individual's standpoint, is 'a safeguard to his or her informational self-determination'.[65] Zanfir claims that this GDPR right amounts to an accentuated or strengthened right to informational self-determination.[66] To have a reflective review of this mainstream perception, the next section traces back to the origin of the right to informational self-determination in the German *Population Census* judgment and have some reflections upon its impact on the development of data protection law.

## 1. The *Population Census* Judgment

The German *Population Census* judgement has been widely seen as a source of inspiration for the development of data protection rules in other Member States as well as at the Union level.[67] In this judgment, the Census Act of 1982, which made provisions for a general census of the population in the spring of 1983, was challenged before German Federal Constitutional Court. To statistically support the census, the 1982 Act required the collection of a wide range of information on the 'recent state of the population, its geographic distribution and composition in terms of demographic, economic and social characteristics'. [68]

While the Federal Constitutional Court found the Act to be 'essentially in compliance with the Basic Law', it invalidated certain provisions concerning 'cross-checks with population registers and the power to transfer data for administrative enforcement'.[69] Notably, a fundamental right to informational self-determination was articulated for the first time in the German constitutional order. The Court held that this right should enable the individuals to decide

[65] Bart Custers and Helena Uršič, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law 4, 11.
[66] Zanfir (n 38) 152.
[67] BVerfGE 65, 1.
[68] Jürgen Bröhmer, Clauspeter Hill and Marc Spitzkatz (eds), *60 Years German Basic Law: The German Constitution and its Court - Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights* (Konrad-Adenauer-Stiftung e.V. 2012) 145.
[69] ibid.

whether to 'engage in or desist from certain activities, including the possibility of actually conducting themselves in accordance with their decisions'.[70]

Interestingly, several lines of reasoning in this judgment may shed some light on how the notions of data protection and data portability have evolved in Europe. First, the German right to information self-determination has a dual legal basis in German basic law: Art 2.1 concerning the free development of personality and Art 1 on human dignity. Second, the right to informational self-determination is not an absolute right. It can be restricted if balanced against other rights or interests.

At that time, there was no specific right concerning data protection and reuse in German jurisdiction. As a result, the Court grounded its reasoning on the 'fall-back right of Art 2.1', which was initially developed in the *Elfes* decision.[71] Art 2.1 of German Basic Law states that

*Every person shall have the right to free development of his or her personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law*[72]

Enders argues that, in essence, Art 2.1 protects the general freedom of action (allgemeine Handlungsfreiheit), that is, the freedom to do whatever one wants, which is limited only by the equal freedom of every other person.[73] Further, Eberle contends that the German law's 'free unfolding of personality is comprehensive and multi-faceted'.[74] There are mainly two dimensions of personality according to German law: the freedom of action and the personal private sphere. Whereas the freedom of action is outward in focus, allowing one to define himself or herself in relation to society, the personal sphere in

[70] ibid 147-8.
[71] ibid 143. See also BVerfGE 6, 32.
[72] Deutscher Bundestag, *Basic Law for the Federal Republic of Germany* (German Bundestag, first published in May 1949) 15.
[73] Christoph Enders, 'The Right to Have Rights: The Concept of Human Dignity in German Basic Law (2010) 2(1) Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD) 1, 4.
[74] Edward J. Eberle, 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33(3) Liverpool Law Review 201, 210-1.

inward in orientation, where one can retreat into and then concentrate on inner development.[75]

It is important to note that the German jurisprudence relates the fundamental right of external freedom closely to human dignity. Based on Arts 1-2, a general right of human personality (allgemeines Persönlichkeitsrecht) has been recognised. As Enders puts it, this indicates that 'the external freedom of the individual is based on internal preconditions'.[76] The right to informational self-determination, expressed in the *Population Census* case, indeed sets foot on both Articles of German Basic Law.[77]

Human dignity and personality are malleable concepts closely connected. As expressed in the *Life Imprisonment* Case, 'the intrinsic dignity of each person depends on his or her status as an independent personality'.[78] With regard to their relationship, Eberle notes that unlike human dignity, personality is 'not an objective value' and comes into play only when 'action is not protected by a more specific right'.[79] Therefore, human dignity interacts with personality in German Basic law to 'form comprehensive protection of human personality and personhood'.[80]

The fact that the safeguards of human dignity restrict an individual's external freedom (free development of personality) implies that one's self-determination has its limitations. As the German Constitutional Court expresses in its judgment:

*The guarantee of this right to "informational self-determination" is not entirely unrestricted. Individuals have no right in the sense of absolute, unrestricted control over their data; they are after all human persons who develop within the social community and are dependent upon communication. Information,*

[75] ibid.
[76] Enders (n 51) 4.
[77] Bröhmer and others (n 46) 148.
[78] BVerfGE 45, 227-28.
[79] Eberle (n 52) 210.
[80] ibid.

*even if related to individual persons, represents a reflection of societal reality that cannot be exclusively assigned solely to the parties affected.*[81]

Schwartz points out that the German Court rightly acknowledged the value of informational self-determination, but failed to 'provide a scale of values for the identifying of interests and assigning of weight to them'.[82] Perhaps this is the reason why the German right has been, as Rouvroy and Poullet point out, misunderstood as 'a sort of alienable property right' under the pervasive influence of possessive individualism.[83] The *Population Census* judgment was, however, deeply rooted in German Constitutional Tradition and hence fundamentally distinct from more recent debates on commodification and inalienability of personal information. It is on this ground that Rouvroy and Poullet negated the connection between informational self-determination with the data-as-property narrative.[84] In a similar vein, Schwartz notes that the German court did 'neither create property interest nor grant exclusive control to an individual'.[85] Rather, the Court compelled the State to organise data processing in a way that personal autonomy would be respected.[86]

What can be gleaned from the German case is that the Court primarily sought to 'create an inner, intimate sphere so that a core of personality might be developed and protected'.[87] Nevertheless, it is essential to note that an individual's external freedom is essentially what this right aims to promote. Bröhmer argues that free development of personality has been construed broadly, and that 'any state action affecting individuals in a negative way by reducing the sphere of individual freedom must be measured against Art 2.1'.[88]

---

[81] Bröhmer and others (n 46) 148.
[82] Paul Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37(4) American Journal of Comparative Law 675, 701.
[83] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth and others (eds.), *Reinventing Data Protection?* (Springer 2009) 50-1.
[84] ibid.
[85] Schwartz (n 60) 690.
[86] ibid.
[87] Eberle (n 52) 210.
[88] Bröhmer and others (n 46) 143.

The observations above cast light on how data protection emerges in EU legal order and recently evolves in the GDPR. As a safeguard of human dignity, the Data Protection Directive entails a number of subject rights for corrective purposes. It did not, it is argued, adequately reflect the parts of external freedom of an individual (*i.e.* free development of personality) that go beyond human dignity.

## 2. The German Impact on European Data Protection Law

The far-reaching influence of this German precedent on the development of data protection in Europe has been well documented. Schwartz points out the 1983 decision had 'exerted' pressure on federal and state legislatures to pass laws that will conform data use to constitutional standards'.[89] It was epitomised by, for instance, the intense debates in German academia as well as the documents prepared for the Federal data protection law in Germany.[90]

Beyond German jurisdiction, Koops argues that the notion of informational self-determination has 'informed the development of data protection law in important ways'. [91] Bygrave notes that the right to informational self-determination has 'a considerable impact on the development of data privacy law and policy in Germany and to a lesser extent, other European countries'.[92] Hornung and Schnabel contend that several foundational principles in the Data Protection Directive, such as data minimisation, purpose limitation and proportionality, can all find their roots in the German decision.[93]

To start with, the idea of informational self-determination was not explicitly expressed in the text of the Directive. One may argue that it has been

[89] Schwartz (n 60) 698.
[90] ibid 687.
[91] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 251.
[92] Lee Bygrave, 'Privacy Protection in a Global Context – A Comparative Overview' (2004) 47 Scandinavian Studies in Law 319, 323.
[93] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25(1) Computer Law & Security Report 84, 87.

materialised by the consent mechanism as well as a body of subject rights. For data subjects, the legal tools given come down to a rectificatory scheme for safeguarding their dignity against harms/or risks arising from the processing of their personal data. As per Art 6(1)(d), the data controller should take steps to ensure that 'data which are inaccurate or incomplete are...erased or rectified'.[94] In connection to this, Art 12 prescribes that data subjects have the rights to access, rectify, erase or block their personal data.[95] All these rights, even implemented in full, do not extend a data subject's control (external freedom) to determining the purpose of data processing. In any event, the data subject is, according to Art 2(a), not in a position to determine the purpose, methods and harvesting of data processing (the role of data controller). Should it be the case, it would be in clear violation of Art 2(d), concerning the foundational dichotomy of data subject/controller. In the Directive, the subject rights given are therefore confined to the aim of rectifying the implications of data processing.

The new GDPR explicitly recognises the value of informational self-determination through its preferred notion of individual control over personal data. Recital 7 states that natural persons should 'have control of their personal data'. [96] As Lynskey contends, the exact wording of 'informational self-determination' is not used in the GDPR because it represents 'the specificities of [German] domestic legal order'.[97] Adopting this German notion within an EU instrument would 'impose the values of one Member State onto the Union as a whole'.[98]

Despite the terminological difference, the new Regulation has strengthened the consent mechanism, requiring it to be 'freely given, specific, informed and unambiguous'.[99] Further, it has inherited the Directive's whole body of subject

[94] Data Protection Directive, Art 6(1)(d).
[95] Data Protection Directive, Art 12.
[96] GDPR, recital 7.
[97] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 179.
[98] ibid.
[99] GDPR, recital 32.

rights, including the rights to information (art 13-14), right of access (art 15), right to rectification (art 16), right to erasure and to be forgotten (art 17), right to restriction of processing (art 18), and right to object (art 21-22). Whereas all these rights primarily serve a rectificatory purpose, the new right to data portability, established in Art 20, can be an exceptional case. By encouraging data subjects to control their personal data and change their preference of data processing, this right to data portability is designed to facilitate flows of personal data across systems, and even across geographical borders.

In connection to the German precedent, data portability appears more akin to the free development of personality than to human dignity. As Zanfir puts it, the right to data portability may be alternatively grounded on the 'free development of dignity personality'.[100] Lynskey contends that it would be challenging to justify data portability on the basis of safeguarding human dignity.[101] This is true because the right diverges from the rectificatory rationale and may be better understood as having a redistributive effect.[102] In any event, the new GDPR right would barely have any impact on the original copy of data still in the incumbent system under the control of the data controller. As recital 68 states, the right to data portability 'should not imply the erasure of personal data'.[103] Consequently, this right creates a parallel world of data processing, and potentially puts the data subject into the role of controller! In this dominant position, data subjects can either reuse their personal data for their own benefits or channel them towards alternative systems of their own choice. Tele and Polonetsky contend that businesses should be ready to share the access and benefits of Big Data with individuals so that they can use data in a tangible

[100] Zanfir (n 38) 151.
[101] Lynskey (n 75) 99, 129.
[102] The division between rectificatory and distributive justice can be traced back to as early as Aristotle's Nicomachean Ethics. See Aristotle, *The Nicomachean Ethics* (David Ross tr, OUP 2009) 86. This dichotomy, indicating the divide between two distinct regulatory mind-sets, has a significant impact on the development of legal doctrines. See, for instance, Peter Benson, 'The Basis of Corrective Justice and Its Relation to Distributive Justice' (1992) 77(2) Iowa Law Review 515. Gregory Keating, 'Distributive and Corrective Justice in the Tort Law of Accidents' (2000) 74 Southern California Law Review 193.
[103] GDPR, recital 68.

way, through what they call ‘featurization’ or ‘application’ of privacy.[104] This benefit-sharing logic has been endorsed by the European Data Protection Supervisor, who argues that if the business would use personal data for secondary purposes, they should also ‘be prepared to share the wealth...with those individuals whose data they process’.[105]

With data portability in place, the GDPR diverges from the Directive by recognising the data subject’s active freedom in relation to data processing. In connection to the German case, the provision of a right to data portability enriches the notion of individual control, allowing it to develop a new dimension featuring free development of personality. In sum, there are two paradigms of control in the GDPR: Whereas consent and all conventional rights are primarily devised to safeguard human dignity (*control for data protection*), the new right to data portability extends to other aspects of personality, allowing for data access, transmission and reuse (*control for data reuse*). This is not to argue, however, that the new right cannot serve rectificatory goals. As will be shown in Chapter 6, the right to data portability can be rectificatory by channelling data flows into user-centric technological systems.

Apart from the legitimacy issue, this chapter also looks at how this new right interacts with conventional rights, *e.g.* right of access (art 15) and right to erasure (art 17), and the new principle of data protection by design and by default (art 25).

[104] Omer Tene and Jules Polonetsky, ‘Big Data for All: Privacy and User Control in the Age of Analytics’ (2013) 11(5) Northwestern Journal of Technology and Intellectual Property 239, 242-3, 264, 268.
[105] European Data Protection Supervisor, ‘Opinion on Meeting the Challenges of Big Data: A Call for Transparency, User control, Data Protection by Design and Accountability (Opinion 7/2015, 19 November 2015) 12.

## III. The Compatibility and Added Value of the New GDPR Right: Towards an Explanation

From the outset, the new right to data portability is in tension with the right of access and the right to erasure.[106] Whereas the former is already in place to facilitate individual access to personal data, the right to erasure may be used (by other data subjects) to prevent data flows out of a processing system.

The new right's overlapping with the right of access as well as the conflict with the right to erasure have all been documented in scholarly literature. Peter Hustinx, the former European Data Protection Supervisor, argued that the right to data portability is 'basically a specification of the present right to require communication of any personal data'.[107] Similarly, van de Sloot claims that the new right is 'partially based on the [existing] right to obtain the personal data being processed about them'.[108] Apart from that, Lynskey brings to the forefront the case where 'a photograph of two friends is ported from one social networking site to another in a way that violates the second individual's privacy rights'.[109] Similarly, the Centre for Information Policy Leadership, a US-based think tank, casts light on whether an individual account holder should be able to download data of other people underneath the account (such as family members' data).[110] The rest of section analyses the new right's compatibility with the existing ones, and further explores the strategies for using these 'micro-rights' in a holistically and coherently manner.

[106] To note, rights to rectification, to restriction of processing and to object merely restrict data processing in different ways, but do not remove data out of the processing system. Therefore, they are not in tension with data portability.
[107] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (EDPS, 14 September 2015) 31-2.
[108] Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307, 315.
[109] Lynskey (n 38) 813.
[110] The Centre for Information Policy Leadership, 'Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's Guidelines on the Right to Data Portability' (2016) available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf> accessed 20 January 2018.

### 1. Diverging from the Right of Access

The new right to data portability was not initially conceived as a fundamentally new right but merely as an extension to the existing right of access. For instance, the European Parliament believed that this right aims to further strengthen individual control over personal data on the one hand, and the right of access on the other.[111] The Commission explained the new right 'serves as a precondition and in order to further improve access of individuals to their personal data'.[112] In either case, the relationship between the rights of access and to data portability is analogous to the rights to erasure and to be forgotten. In essence, the GDPR would not create a new right but merely make the existing one more prominent and effective.[113] This conception culminated in the Albrecht report, which formed the basis for the Opinion of the Committee on Civil Liberties, Justice and Home Affairs (LIBE). Rapporteur Jan Philipp Albrecht suggested, among many other changes, the merger between Art 15 (data access) and Art 18 (data portability) of the GDPR proposal.[114] As a result, the entire Article 18 was deleted, and a general right of access and to obtain data was established in this Opinion, without any reference to the term 'data portability'.[115] In a similar vein, Rapporteur Gallo from the Committee on Legal Affairs supported the deletion of Art 18 on the ground that 'this new right...brings no added value to citizens concerning the right of access'.[116]

In numerous meetings of the Working Party on Information Exchange and Data Protection (DAPIX), the concerns that there is no need to introduce a new right where the existing right of access is already in place was also voiced. In July 2012, the Spanish representatives noted that Art 18 of the proposal 'does not

[111] European Parliament (n 37) recital 55.
[112] ibid 9.
[113] European Commission, 'Factsheet on the "Right to Be Forgotten" Ruling (C-131/12), available at <https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf>accessed 29 March 2019.
[114] Albrecht (n 37) 201. See also Cedric Burton, Christopher Kuner, and Anna Pateraki, 'The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report' (2013) 12 Privacy and Security Law Report 1-7.
[115] ibid.
[116] ibid 525.

concern data portability as such but could be seen rather as a specific form of a right of access'.[117] This was indeed a genuine remark taking into account the old framing of the new right in Art 18, which stated that personal data should be provided to the data subject 'in an electronic and structured format that is commonly used'.[118] The Commission was also in an attenuated view that Art 18 is only applicable when the data controller 'has on his or her own accord chosen to use a commonly used format'.[119] As a consequence, Art 18 was designed merely to 'extend the basic law of access by allowing transfer in a more usable format'.[120] To note, machine-readability had not yet been put forward as a legal requirement at that time. In another DAPIX meeting before the Trilogue discussion, the Belgian representatives cast doubts again on the added value of the new right to data portability. French representatives still saw it as inherently related to the right of access.[121]

From the outset, the two rights indeed have many similarities. In spite of the scope of data concerned, both Art 15(3) and Art 20(1) require that the data controller to provide a copy of personal data at the request of the data subject.[122] In the same manner, both Art 15(4) and Art 20(4) stipulate that the GDPR right 'shall not adversely affect the rights and freedoms of others'.[123] These similarities beg the question as to whether the two rights pursue the same objective and whether they are functionally equivalent.

Scholarly efforts have been made to differentiate the new right with the existing right of access. Swire and Lagos, for instance, strongly disagree that the new right to data portability is 'a precondition for further access of individuals'.[124] They argue this right 'goes far beyond existing access requirements' and

[117] Internal Report of the Meeting of the Working Party on Information Exchange and Data Protection (Ares(2019)693034, 11-12 July 2012) 30.
[118] European Commission (n 5) Art 18.
[119] ibid 31.
[120] ibid.
[121] Internal Report of the Meeting of the Working Party on Information Exchange and Data Protection (Ares(2019)693298, 13 March 2013).
[122] GDPR, Arts 15(3) and 20(1).
[123] GDPR, Arts 15(4) and 20(4).
[124] Swire and Lagos (n 38) 369.

should hence be deemed as a distinct right.[125] Primarily, two reasons are put forward in this respect. First, they note that data controllers can narrow down the scope of the subject access request, but cannot do so when dealing with data portability request.[126] Second, the new right requires, to some extent, a technical infrastructure for automatic response to request or transmission of personal data, which is otherwise not seen in the case of subject access request.[127] Lynskey similarly argues that the conception of data portability as a simple extension to the right of access should be dismissed.[128] She points out that the remit of data portability is narrower than that of access: whereas the right of access applies to all personal data, regardless of the legal basis for processing, the scope of 'portable data' is confined to those 'provided by the data subject', being processed on the basis of consent or contract.[129]

Apart from these differences identified, it is argued that a more significant difference between the two GDPR rights lies in the requirements of data format for interoperability. Art 20(1) GDPR requires the data controller provide data in a 'structured, commonly used and machine-readable format'.[130] Besides, recital 68 adds that data controllers should be '*encouraged* to develop interoperable formats that enable data portability'.[131] In Chapter 5, it will be explained in detail that these requirements are essential to ensure interoperability, especially on syntactic layer. In contrast, Art 15 (concerning the right of access) is silent on the format in which data should be provided. As the Article 29 Working Party (A29WP) notes, the right of access has been 'constrained by the format chosen by the data controller'.[132] Art 12(1) merely states that any communication with the data subject should be in a 'concise,

[125] ibid 372.
[126] Swire and Lagos (n 38) 370-1.
[127] ibid.
[128] Lynskey (n 38) 812.
[129] ibid.
[130] GDPR, Art 20(1).
[131] GDPR, recital 68.
[132] A29WP (n 40) 4.

transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.[133]

It is argued that a distinction should be made between the two sets of criteria mentioned above. They respectively correspond to the concepts of machine-readability and human readability, derived from the field of computer science. According to the Open Data Handbook, human readability means that data is represented in a format that can be conveniently read by a human.[134] Some human-readable format, such as PDF, are not machine-readable because they cannot be automatically read and processed by a computer.[135] A plain reading of the two sets of GDPR criteria may lead to the conclusion that whereas the right to access facilitates human readability of personal data ('intelligible and easily accessible'), the data portability right mandates the machine-readability of data to facilitate the machine intelligence. As the Commission once rightly puts it, data portability should 'apply specifically for IT applications' whereas the right of access is, in general, a right to get (straightforward) information.[136]

Based on this distinction, the new right should be decoupled from the conventional logic of data access clearly. This right is not designed to make data easily and immediately comprehensible to data subjects. In many cases, machine-readability and interoperability require, quite the opposite, a full set of technical, raw and complex datasets that do not make any sense to an average individual unless further processed. The new right to data portability marks a step towards another direction, mandating technical specifications that support data analysis, transmission and reuse. This would unleash the enormous value of personal data, extractable only with advanced processing techniques.[137] In

[133] GDPR, Art 12(1).
[134] Open Data Handbook: Glossary, available at <http://opendatahandbook.org/glossary/en/>accessed 21 May 2019.
[135] ibid.
[136] DAPIX (n 95) 3.
[137] Jack Hardinges, 'Will GDPR and Data Portability Support Innovation?' (ODI, 15 February 2018) available at <https://theodi.org/article/will-gdpr-and-data-portability-support-innovation/>accessed 25 May 2019. See also CtrlShift, 'Data Mobility: The Personal Data Portability Growth Opportunity for the UK Economy' (A Report Prepared for the DCMS, 19

due recognition of the transformative powers in big data analytics, cloud computing, artificial intelligence and machine learning, it is reasonable to argue that the new right will bring much more significant value than mere transparency of a certain processing system. As the Centre for Information Policy Leadership (CIPL) contends, data portability right should 'neither replace nor recalibrate other rights'; the use of this new right should 'focus on domains where it effectively has added value'.[138]

### 2. Balancing with the Right to Erasure

The rights to erasure and to data portability are described as 'sibling rights' in the GDPR.[139] This can be epitomised by the fact that these rights are situated in the same section of the GDPR and that there exists in Art 20 (data portability) an explicit reference to Art 17(right to erasure), suggesting that the two rights are somewhat related.

In practice, the two rights may be exercised (by multiple data subjects) in a conflictual manner. This is the case where one data subject seeks the permanent removal of certain personal data whereas another data subject wants to port that data away.

With regard to this potential conflict, it has been argued that The occurrence of GDPR rights in conflict with each other stems from the fact that personal data is interpersonal and relational. As a result, one set of personal data may simultaneously relates to a number of data subjects.[140]

The GDPR has anticipated this situation and entails rules on balancing the rights in conflict. At face value, there appears to be a number of provisions that

---

November 2018) available at <https://www.gov.uk/government/publications/research-on-data-portability>accessed 25 May 2019.

[138] CIPL (n 88) 3.

[139] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why A "Right to An Explanation" is Probably Not the Remedy You are Looking For' (2017) 16(1) Duke Law and Technology Review 1, 72.

[140] Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict between Right to data Portability and Right to Be Forgotten under the General Data Protection Regulation' (2018) 8(4) International Data Privacy Law 309.

could shed light on this issue. Art 20(3) states that the right to data portability (as prescribed in Art 20(1)) shall be without prejudice to right to erasure and to be forgotten (Art 17). This general principle is open to interpretation, and the A29WP Guidelines apply it to the case where only one data subject is involved, who exercises the two rights at the same time. It is stated in the Guidelines that the exercise of the right to be forgotten 'cannot be used by a data controller as a way of delaying or refusing such erasure'.[141] Adhering to this narrow interpretation, Art 20(3) would not apply to the case where one data subject exercises the right to be forgotten while another enforcing the right to data portability on the same set of data. Art 20(4) does not explicitly refers to the right to erasure but generally states that the right to data portability 'shall not adversely affect the rights and freedoms of others'.[142] Recital 68, which accompanies Art 20, suggests that the term 'others' here refer to other data subjects.[143] That so, the GDPR stipulates that the right to data portability make way to other rights in the GDPR when they are in conflict with each other.

Similar provisions can be found in Art 15(4) in which it states that the right of access, an existing data protection similar to the data portability right. In contrast, there exists no such provisions in Art 17, and both the right to data portability and the right of access do not fall into the exceptions to the right to be forgotten, as prescribed in Art 17 GDPR. It is hence argued that there appears to be a hierarchical relationship between GDPR rights, that is, that the right to be forgotten appears higher in rank than the rights to data portability and of access.[144] This is not to argue, however, that the RtBF should categorically override other subject rights in conflict. The tension between the right to be forgotten and the right to erasure, as argued elsewhere, reflects a longstanding tension between access to information and third-party privacy.[145] The balancing of two GDPR rights could therefore be aligned with existing legal frameworks as well as case-law. In this regard, the *Google Spain* judgment is

[141] A29WP (n 37) 7.
[142] GDPR, Art 20(4).
[143] GDPR, Recital 68.
[144] A Tale of Two Rights (n 118) 313.
[145] ibid 314.

particular germane as it dealt with the balancing between economic interests of a search engine and the right to erasure as prescribed in the Data Protection Directive.[146] The CJEU held that the right to erasure cannot be justified by merely the economic interest which the operator of an engine has in the processing [of personal data]'.[147] However, an interference with the right to erasure may be justified by certain reasons, such as 'the preponderant interest of the general public in having access to the information'.[148] Applying this rationale to the conflict between two GDPR rights, it is argued that the right to be forgotten prevail over the right to data portability as applied to promote individual economic interests. However, there could be some grounds on which the Court favours data portability over erasure, bearing in mind the wide-ranging, multidimensional impacts of data portability. For instance, Art 20 can be enforced purely for better controlling and managing personal data by transmitting data from the incumbent controller to a personal data store. Additionally, the right's impacts on competition, despite that the right is not devised for this purpose, should also be taken into account when the Court balances conflicting rights.

### 3. Combined Use of GDPR Rights: Towards Strategies for Data Subjects

Each subject right mentioned above is a 'micro-right' that micro-manages the processing of personal data in a specific way, whether it be transparency, rectification, erasure, transmission or objection. The rest of this section further elucidates on the possibilities of jointly and strategically exercising these rights together. This holistic approach has already been implied in both policy-making documents as well as in the scholarly literature. For instance, the European Data Protection Supervisor (EDPS) argues that the new right to data portability reinforces existing rights and should be particularly connected to the right to erasure.[149] Scudiero points to the case where a data subject uses two

[146] *Google Spain* (n 14) para 97.
[147] ibid para 81.
[148] ibid para 97.
[149] European Data Protection Supervisor, 'Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee

rights together, 'requiring the portability of data while asking the data controller to erase [the original copy of] them'.[150] In the Opinion of the Committee on the Internal Market and Consumer Protection's opinion on the GDPR proposal, Rapporteur Lara Comi points out that while the right to data portability does not apply to certain types of personal data, such as internally used outcomes, the right of access is still valid in this respect.[151] The A29WP similarly implies that data subjects can access inferred or derived data, to which the right to data portability does not apply, through the right of access.[152]

In practice, the new right to data portability may indeed interact with conventional rights in a way more complicated than it initially appears. It would be ingenuous to argue that the new right to data portability cannot be used for information purposes. Quite the opposite, the personal data ported, notably in together with metadata, can be more revealing than the redacted information obtained through Art 15 GDPR. Similarly, it is contestable that data obtained through Art 15 GDPR in an 'intelligible' form is not always machine-processable. The new right to data portability might also be used in together with the right to erasure to the effect of taking data entirely out of a processing system. Three strategies about the joint use of GDPR rights are detailed below.

First, the rights of access and to data portability can be used jointly to enlarge the scope of personal data obtained. Whereas Art 20 applies only to data provided by the data subject, according to Art 20(1), Art 15 may be of use to give access to derived and inferred data (*i.e.* data created by the data controller based on 'the data provided by the data subject').[153] Scudiero notes that a data subject may exercise his or her right of access to 'obtain a copy of inferred data...thus circumventing the legal limitations to the right to data portability'.[154]

---

and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union' (EDPS Opinion, 14 January 2011) 19.
[150] Lucio Scudiero, Bringing Your Data Everywhere: A Legal Reading of the Right to Portability (2017) 3 European Data Protection Law Review 119, 126.
[151] Albrecht (n 37) 418.
[152] A29WP (n 40) 10.
[153] ibid.
[154] Scudiero (n 123) 123.

However, the quality of data obtained in this way may be compromised as they are not all machine-readable by default. This combined use of GDPR right may therefore be useful for information purpose only.

Second, the right of access can be used to inform the implementation of data portability and arguably vice versa. As the A29WP suggests in its Guidelines, if a data subject has doubts on the compliance with the right to data portability, the further request for data access, if any, should be fully responded.[155] In this context, the right of access can be particularly useful to understand what types of data to port and whether the data controller has adequately responded to the request.

In addition, the right of access is limited in the sense that the data controller may request to specify the information requested, and narrow down the scope of data provided.[156] In *YS and Others*, for instance, the CJEU held that it is sufficient to provide the data subject with a full summary of personal data, as opposed to the data itself.[157] The Court reasoned that this enables the data subject to become aware of those data and check if they are accurate. Consequently, it is not just machine-readability that is affected, but also the comprehensiveness of data. Further, the usefulness of that 'data' is highly contingent on the decision made by the controller, concerning what to present about the 'black box' (processing system). The information, being redacted, summarised and selected by the controller, is less likely to provide a full view of the processing system concerned.

The right to data portability, which can be useful for information purposes as well, would complement the right of access in this respect. It covers the individually provided data that the data controller shall provide in full (without

[155] A29WP (n 40) 7.
[156] GDPR, Art 12. See also Information Commissioner's Office, 'Subject Access Code of Practice: Dealing with Requests from Individuals for Personal Information' (version 1.2, 9 June 2017) 40.
[157] Joined Case C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* ECLI:EU:C:2013:838, para 60.

redaction), and arguably including raw data observed from the activities of users.[158] Ideally, a full set of metadata would objectively reveal the way personal data is organised and used for what purpose in a specific processing system. These data are less likely to be affected by the controller's deliberate redacting and could reveal unanticipated findings that are otherwise unattainable through Art 15 GDPR.[159]

Third, the right to data portability does not automatically imply the erasure of personal data in the incumbent system.[160] Therefore, the combined use of the rights to data portability and to erasure may be necessary when a data subject intends to switch to another processing service. It appears that the two rights converge around the processing of personal data based on consent or performance of a contract. As per Art 20(1), the right to data portability applies only to the processing of personal data based on consent or contract.[161] Art 17(1) also prescribes that the right to erasure applies after the data subject withdraws consent (point (b)) or when the personal data is 'no longer necessary in relation to the purpose for which they were collected or otherwise processed' (point (a)).[162] If certain datasets are being processed on the basis of consent[163], the data subject may withdraw consent first and exercises his or her rights to erasure and to data portability as a necessary follow-up. In the case where the processing of personal data is based on the performance of contract[164], the data subject is also able to enforce his or her right to data portability. The erasure of data is, however, subject to the proviso that he or she resorts to remedies, for instance, in consumer protection law, to terminate the contract. Upon termination of the contract, the data subject may claim,

[158] A29WP (n 40) 9-10.
[159] For instance, in my Twitter archive requested on 25 May 2018 and obtained the following day, there exists not merely what I have provided on Twitter, but, to my surprise, my profile created by Twitter for advertising purposes, which contains many inaccurate labels.
[160] GDPR, recital 68.
[161] GDPR, Art 20(1).
[162] GDPR, Art 17(1).
[163] GDPR, Art 6(1)(a).
[164] GDPR, Art 6(1)(b).

pursuant to Art 17(1)(a), that the processing is 'no longer necessary' and exercises his or her right to erasure.[165]

While a joint use is theoretically possible, these rights are subject to different sets of conditions and exceptions and apply to a different scope of data. In addition to that, there are legitimate bases other than consent and contract on which processing of personal data can be legitimized.[166] The issue of how these rights may be used in together needs to be empirically examined and, given the inconsistencies mentioned above, this may at best be effective in limited circumstances.

## IV. The Clash with Data Protection by Design and By Default: A Dilemma of Trust

The last section of this Chapter deals with the issue that the right to data portability is likely to clash with the new principle of data protection by design (DPbD) with consequences of different degrees. Apart from data portability, the GDPR also introduces a new principle of data protection by design and by default in Art 25 GDPR.[167] Basically, this lengthy article introduces, as Bygrave puts it, 'a qualified duty' for the data controller to put in place technical and organisational measures for 'implementing data protection principles' on the one hand, and 'ensuring data protection rights' on the other.[168]

The GDPR principle of DPbD has been ostensibly inspired by the nominal concept of Privacy by Design, coined by Ann Cavoukian, the previous Information and Privacy Commissioner of Ontario.[169] Cavoukian argues that privacy must be embedded into technologies, operations and architectures by default, preventing invasive events *ex ante*.[170] Apart from this origin, 'Privacy-

[165] GDPR, Art 17(1).
[166] GDPR, Art 6(1).
[167] GDPR, Art 25 GDPR.
[168] Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 Oslo Law Review 105, 114.
[169] Cavoukian (n 15) 1.
[170] ibid 1-3.

Enhancing Technologies' (PETs) is provisionally an equivalent notion has been widely used in a technical context.[171] These concepts are closely related but have been derived from different contexts and feature different objectives, methods and priorities. For instance, Veale and others note that the PETs narrative takes 'single-minded aim at information disclosure and risks' in contrast to the multifacetedness of PbD or DPbD principles.[172] According to Art 25, the DPbD appears to be predominantly situated in the contexts of pseudonymisation and data minimisation.[173] While the principle is supposed to 'protect the rights of data subjects' and enable the data subject to 'monitor' the data processing, it has not yet extended to, for instance, facilitating the infrastructural design for making data portable or interoperable between processing systems, pursuant to Art 20(2) GDPR.[174]

Encouraged by the DPbD, the adoption of measures such as anonymisation, pseudonymisation and encryption would exert an impact on the implementation of his or her data protection rights. As the de-identification process is sometimes irreversible, data controllers would be reluctant to or incapable of re-identify a data subject merely for complying with data protection rights. What is worse, Veale and others identify the risks that these difficulties in re-identification are mostly trivial for adversaries, who have 'high tolerance for inaccuracy and access to many additional, possibly illegal, databases'.[175] Therefore, data controllers may 'bind their own hands' by deploying technical measures encouraged by the DPbD.[176]

Diaz and others note that informational privacy law interestingly bridges two distinct trust paradigms: there is one assuming that data controllers are trusted

[171] Claudia Diaz, Omer Tene and Seda Gürses, 'Hero or Villain: The Data Controller in Privacy Law and Technologies' (2013) 74(6) Ohio State Law Journal 923.
[172] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8(2) International Data Privacy Law 105, 107.
[173] GDPR, Art 25.
[174] GDPR, Art 20(2).
[175] Veale and others (n 145) 107.
[176] ibid.

third parties and the other treating them with suspicion and distrust.[177] Further, the legal framework has recently shifted from focusing data minimisation (through PETs) to 'imposing information stewardship obligation on data controllers who are increasingly viewed as custodians of individuals' rights'[178] In contrast, the technological community specialising in PETs still 'proceeds from a diametrically opposed perception', not of the data controller as a trusted third party, but as an adversary.[179] Consequently, the tension between the two parts of data privacy law is inevitable to grow.

Despite this paradigmatic clash, it is argued that the use of de-identification measures would have a more immediate impact on the right to data portability. Apart from the *static* scope of portable data defined by law, technical measures such as anonymisation, pseudonymisation and encryption would create a *dynamic* scope of personal data to which the GDPR right applies in a given case.

Anonymisation, which is not explicitly defined in the GDPR, generally refers to a technical method to make data 'non-personal' (that is, unlikable to a natural person). It is a technique that removes personally identifiable information from a dataset to the effect that the data subject that information is concerning remains anonymous. Recital 26 states that anonymous data include those 'not relating to an identified or identifiable natural person' by nature and data that have been rendered anonymous.[180]

Whereas anonymisation irreversibly prevents identification, pseudonymisation, another attenuated technique for identity removal, makes data temporarily unlinkable. According to Art 4(5), pseudonymisation is a technique that 'makes data no longer attributable to a data subject without the use of additional information'. [181] Also known as keys or artificial identifier, this additional

[177] Diaz and others (n 144) 963.
[178] ibid.
[179] ibid.
[180] GDPR, recital 26.
[181] GDPR, Art 4(5).

information is not often held by the data controller. In so doing, the controller may exempt itself from the obligation to respond to subject requests for pseudonymised data.[182]Encryption is not a technique for de-identification per se but has often been used as an excuse not to comply with subject rights in practice. It is defined as a protection measure that renders the personal data 'unintelligible' to any person without authorised access.[183]

Encryption would obstruct the implementation of subject rights because it renders it difficult to 'tie-back personal data to data subjects on demand'.[184] This is especially true for advanced encryption techniques such as end-to-end encryption, which ensures that no one (even including the provider of communication service) can read the message except the sender and the receiver.[185]

Data protection rules do not apply to anonymous data, so there is no dispute that this type of data falls out of the scope of data portability.[186] It is contested, however, whether the right to data portability can and should apply to pseudonymous or encrypted data. The A29WP is in a view that pseudonymous data falls within the scope of Art 20 as they 'can be clearly linked to a data subject'.[187] The data controller concerned cannot, therefore, 'refuse to act on the request for exercising subject rights' should the data subject provide additional information for re-identification.[188] In this case, the controller may still refuse to respond on the ground that he is 'not in a position' to identify the data subject.[189] In this respect, Veale and others argue that the burden of proof for the controller would be very high in light of the GDPR's 'emphasis on

[182] GDPR, Art 11(2).
[183] GDPR, Art 34(3)(a).
[184] Application for Access to Documents - Ref GestDem No 2018/1669, Digital Europe.
[185] Andy Greenberg, 'Hacker Lexicon: What is End-to-end Encryption?' (WIRED, 25 November 2014) available at <https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>accessed 26 May 2019.
[186] GDPR, recital 26.
[187] A29WP (n 40) 9.
[188] GDPR, Art 12(2).
[189] GDPR, Art 11(2).

accountability and weightier focus on responsibilities'.[190] As per Art 11(2), the data subject may provide additional information to enable identification, and the controller is not allowed to refuse in that case.[191] Digital Europe contends that this would be 'a retrograde step for privacy' because it creates a disincentive for data controllers to hold pseudonymous data.[192] Indeed, before deploying pseudonyms, it is advisable for data controllers to think about the consequences of not comply with subject rights. While technical solutions have been suggested, *e.g.* creating a parallel system for compliance[193], this would be a slow transitional process on the condition that data controllers would be willing to take extra costs.

With regard to encryption, the GDPR has failed to acknowledge the tension between data security and subject rights fully. Apple, for instance, uses this type of encryption to protect iMessage and FaceTime conversations and the company hence claims that 'there is no way for us to decrypt your data when it is in transit between services'.[194] This means that 'no one but the sender and receiver can see or read them', and Apple uses this as a reason not to provide certain categories of user data to law enforcement, users and any other group.[195]

Indeed, the adoption of de-identification and encryption measures may not necessarily prevent data subjects from exercising their right to data portability. Nevertheless, the deployment of these measures would place the data controller in an awkward position to respond to subject rights. As DPbD encourages their adoption, data controllers may legitimately restrict the scope of portable data on these grounds in practice.

---

[190] Veale and others (n 145) 116.
[191] GDPR, Art 11(2).
[192] Digital Europe (n 157).
[193] Veale and others (n 145) 114-6.
[194] Apple, 'This is How We Protect Your Privacy' available at <https://www.apple.com/uk/privacy/approach-to-privacy/>accessed 8 May 2019.
[195] 'Apple's Commitment to Customer Privacy' (16 June 2013) available at <https://www.apple.com/apples-commitment-to-customer-privacy>accessed 2 August 2018.

## Conclusion

This chapter lays the groundwork for the fundamental inquiry of the thesis that how data portability furthers the objective of data protection. It primarily examines the legitimacy of introducing a right-based data portability scheme in the new data protection framework. The GDPR now emphasises individual control over personal data as a normative preference, thereby providing a legal basis for introducing the new right to data portability. The Chapter further inspects the EU notion of control by exploring its conceptual link with the right to informational self-determination, initially expressed in the German *Population Census* judgment. It is argued that whereas the Data Protection Directive narrowly focused on human dignity, the GDPR has extended one's self-determination (through data portability) to data access, transmission and reuse, thereby giving expression to the free development of personality. Echoing the dual basis of informational self-determination, the GDPR enables two forms of control: whereas consent and the rights inherited from the Directive jointly enable *rectificatory control*, the new right represents a distinct form of control with influence on the asymmetries of data power, what this paper calls *redistributive control*.

The chapter also looks at whether the new GDPR right is compatible with the existing rights, as well as the principle of DPbD recently introduced into the EU data protection framework. It is noted that some schemes are in clear tension with data portability. First, the right to erasure may be used against the flow of personal data out of a processing system. Second, technical measures such as anonymisation, pseudonymisation and encryption could have an impact on the implementation of subject rights. While these counterforces do not necessarily make subject rights impractical, the scope of personal data concerned would be significantly restricted as a result. In addition to the *static* scope of personal data defined by the GDPR, this chapter suggests a *dynamic* scope dictated by technical measures adopted for data protection. These technical hurdles would indeed stand as an enduring hurdles to effective use of the GDPR rights. Given that the GDPR permits such tension to exist in the

years to come, there should be a call for designers to reconcile the tension through better design of processing systems.

Last, attempts have been made to articulate the added value of the new right to data portability. To start with, the right should be clearly distinguished from the right of access. Whereas the latter provides human-comprehensible information, the former innovatively focus upon machine readability for new opportunities mediated by technology. Further, the right to data portability should not be viewed in isolation. In most cases, this right can and should be used in tandem with other rights in data protection framework. It has been shown that the rights of access and to data portability can be jointly used in a mutually reinforcing way. Further, the right to erasure might be jointly used to the effect that a data subject takes his or her personal data completely out of a processing system. Strategies for using these micro-rights effectively and holistically are indeed necessary to overcome the shortcomings of the data micro-management prompted by the GDPR. It is argued that guidelines should be provided by data protection authorities, not only to data controllers for compliance, but also to data subjects who need additional assistance to use their rights wisely.

Apart from data protection, the EU data protection law has another objective, *i.e.* free movement of personal data in the European Union. The next chapter will explore whether the right to data portability can alternatively hinge upon this economic objective and justifiably pursue the normative goal of consumer welfare.

# Chapter 3 Navigating the Right to Data Portability at the Intersection of Data Protection, Consumer Protection and Competition Law in the EU

## Introduction

It was argued in Chapter 2 that the new right to data portability is not inherently about data protection. By empowering the individual with the ability to access, transmit and reuse data, it directly facilitates the economic welfare of that individual, thereby enabling a new paradigm of control, what this thesis calls *redistributive* control. Indeed, this GDPR right appears more akin to the other objective of data protection law – that is, the free flow of personal data. This economic objective used to be fulfilled passively through the harmonisation of laws of the Member States in the EU. With data portability in place, it might be achieved by the increased flow of data between processing systems led by data subjects.

The GDPR right was introduced at a time when three areas of EU law - consumer protection, data protection, and competition law - were bleeding into each other. New schemes similar to the right to data portability are being or have been introduced in other areas of law, facilitating normative goals other than data protection. This convergence of EU law begs the questions as to whether the GDPR's emphasis on individual control can be aligned with consumer welfare, an overarching value that both consumer protection and competition law pursue. At a granular level, it is also worth exploring whether the GDPR right should be integrated with, or differentiated from, its counterparts in other areas of law.

Beyond data protection, this chapter examines the right to data portability at the intersection of EU law. It inquires whether this new right can be alternatively grounded on the economic objective of data protection law, the free movement of personal data. As the EU law convergence continues to expand, this chapter

also explores whether the right can legitimately and instrumentally pursue the goals of consumer protection and competition law.

The chapter is divided into two parts. In view of the EU law convergence, part 1 examines whether the new GDPR right may justifiably pursue normative goals such as competition and consumer welfare. It is argued that with data portability at play, the hybrid notion of individual control in the GDPR may be aligned with the overarching goal of consumer welfare. It prompts a rethinking of EU data protection, its objectives and instruments, as well as the interplay with other interrelated areas of law. Part 2 examines whether the right is capable of instrumentally facilitating switching or alleviating lock-in. While the right by itself falls short of freeing consumers from a particular service, it has recently been complemented by the new scheme in the Digital Content Directive (DCD). The debates on the right's potentials and limitations should, therefore, be revisited in a broader legal landscape.

## I. A Trio of EU Law: Commonality, Difference, and Convergence

EU rules on data protection, consumer protection, and competition are highly connected with, but also subtly distinct from, each other. Recently, a convergence between these areas of law is taking shape, and schemes similar to the GDPR right to data portability are being or have introduced in the EU legal order. In this time of convergence, it is worth inquiring (1) how the data protection objective of individual control over personal data may be aligned with consumer welfare, an overarching value that both consumer protection and competition law pursue and (2) whether the GDPR right should be integrated or differentiated with new data portability regimes.

### 1. Common Grounds

EU rules on data protection, consumer protection, and competition law are highly interrelated. As the European Data Protection Supervisor (EDPS) puts

it, they share the same goals of promoting growth, innovation, and the welfare of individual consumers.[1]

EU Competition law is primarily concerned with market efficiency. Wesseling notes that this area of law has gone through several stages of evolution over the past few years. Initially, competition law functioned as 'a means of preventing public obstacles to interstate trade' and now endeavours to 'ensure necessary controls of corporate mergers and liberation of sectors of the public economy'.[2] Notably, competition law in the EU has arguably associated with the rationale of consumer welfare.[3] While the Court of Justice of the European Union (CJEU) is reluctant to recognise consumer welfare as a goal of competition law [4] , the Commission has explicitly acknowledged that competition law prohibits activities that may harm consumer welfare.[5] Albors-Llorens argues that the notion of consumer welfare in competition law has been developed in close proximity to market efficiency. Those factors behind the market efficiency, such as increased legal certainty and comparability of offers,[6] are also beneficial to consumers. By tackling the asymmetries of power and information, market efficiency may also have a desirable impact on consumer welfare.

[1] 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' (Preliminary Opinion, March 2014) 3.
[2] Rein Wesseling, *The Modernisation of EC Antitrust Law* (Hart Publishing 2000) 48-9.
[3] Neil Averitt and Robert Lande, 'Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law' (1997) 65(3) Antitrust Law Journal 713.
[4] The term consumer welfare has only been used in few cases without recognising it as a goal to be pursued. Case T-168/01 GlaxoSmithKline Services Unlimited v EC Commission [2006] ECR II-2969, para 256. Case T-201/04 Microsoft Corp v EC Commission [2007] 5 CMLR 11, para 41. Case C-53/03 Synetairismos Farmakopoion Aitolias & Akarnanias (Syfait) and Others v GlaxoSmithKline plc and GlaxoSmithKline AEVE [2005] ECR I-4609, the Opinion of Advocate General Jacobs, paras 91-2. See also Pinar Akman, '"Consumer Welfare" and Article 82EC: Practice and Rhetoric' (2009) 32 World Competition Law and Economics Review 71.
[5] European Commission, Communication from the Commission — Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings OJ C 45, 24.2.2009, Art 19.
[6] ibid para 5.

In contrast, the EU consumer protection law promotes the welfare of consumers in a different manner. Traditionally, consumer welfare is safeguarded by restrictions on contractual freedom to the effect that there is no need for consumers to engage actively. Apart from this, EU consumer protection law is recently characterised with an emphasis on consumer empowerment. For instance, the 2007-2013 Consumer Policy recognises the utmost importance of consumer welfare in relation to 'price, choice, quality, diversity, affordability, and safety'.[7] In a more recent programme for the years 2014-20, the EU aims to empower citizens to 'play a full part in the internal market' by providing them with 'sufficient tools, knowledge and competence' and by raising consumer awareness.[8]

EU data protection law does not squarely fit this narrative of consumer welfare. As stated earlier, it has as its objectives the protection of personal data as well as the free movement of personal data in the Union.[9] This law can indeed be seen as a regulatory response to the market failure of competing on privacy and data protection but has never explicitly recognised consumer welfare as a goal to be pursued. Traditionally, the EU data protection regime was primarily concerned with the dignitary aspects of individual welfare. The subject rights given are rectificatory by nature and useful only for safeguarding human dignity against harms arising from data processing. Established upon the dichotomy of the data subject/controller[10], this Directive has never allowed the individuals (data subjects) to determine the purpose, method, and harvesting of data processing.[11] This dignity-based conception should be, however, revisited in the era of GDPR. The new right to data portability now allows the data subject to reuse personal data for their own benefits, thereby directly promoting his or

[7]Decision No 1926/2006/EC of the European Parliament and of the Council of 18 December 2006 establishing a programme of Community action in the field of consumer policy (2007-2013) OJ L 404, 30.12.2006, p. 39–45.

[8] Regulation (EU) No 254/2014 of the European Parliament and of the Council of 26 February 2014 on a multiannual consumer programme for the years 2014-20 and repealing Decision No 1926/2006/EC OJ L 84, 20.3.2014, p. 42–56, recitals 1, 6.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) OJ L 119, 4.5.2016, p. 1–88, Art 1.

[10] GDPR, Art 4.

[11] Data Protection Directive, Art 2(a) and (d).

her economic welfare. Ostensibly, the GDPR's emphasis on individual control (through data portability) might align with the overarching value of consumer welfare.

## 2. Differences in Legal Basis, Regulatory Target and Approaches

At a granular level, EU rules contribute to their shared goals in distinct ways. The most explicit difference lies in the disparate bases for these rules in the Treaty on the Functioning of the European Union (TFEU).[12] Competition law lies at the centre of EU law, and there are numerous Articles of the TEFU concerned with competition. In brief, Arts 101-106 TFEU inhibit agreements that prevent, restrict, or distort competition on the one hand, and prohibit undertakings in a dominant position to abuse their power on the other.[13] Arts 107-109 are concerned with the prohibition of preferential treatment by the Member States.[14] With regards to consumer protection, Arts 12 and 169 jointly require 'a high level of consumer protection' in the EU.[15] EU data protection law now has an independent legal basis in Art 16 TFEU, which states that 'everyone has the right to the protection of personal data'.[16] Further, a new right to protection of personal data is enshrined in Art 8 of the EU Charter of Fundamental Rights, offering additional support for EU secondary law.[17] The Charter also recognises, to a lesser degree, that the Union should 'ensure a high level of consumer protection'.[18] Understandably, competition cannot be framed as a right for the business, but the Charter recognises in Art 16 a freedom to conduct a business.[19]

Apart from the legal basis, the three areas of EU law diverge on their regulatory targets as well. A rough line can be drawn, for instance, between consumer protection and competition law. Averitt and Lande contend that whereas

[12] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390.
[13] TFEU, Arts 101-106.
[14] TFEU, Arts 107-109.
[15] TFEU, Arts 12, 169.
[16] TFEU, Art 16.
[17] CFR, Art 8.
[18] CFR, Art 38.
[19] EU Charter of Fundamental Rights, Art 16.

antitrust law '[ensures] the marketplace remains competitive so that a meaningful range of options is made available consumers', consumer protection law makes it easier for consumers to 'choose effectively from among those options'. [20] Albors-Llorens argues that competition law addresses 'external market failures which may, for instance, reduce the number or quality of the options available to consumers' whereas consumer protection law deals with market failures which are 'internal to consumers and which may prevent them from making rational choices'.[21]

The EU approaches to data protection and consumer protection also have subtle differences. Whereas the latter focuses on consumers and their economic wellbeing, the former primarily looks at personal data and inquires whether it is processed in a lawfully and fairly manner. In terms of the regulatory toolkits, the restrictions on contractual freedom are ostensibly independent of the logic of legitimising the processing of personal data. Further, the fact that certain processing is legitimized does not necessarily ensure that harm does not arise from contractual freedom.

Last, both data protection and competition law address the asymmetries of power in different ways. The former primarily puts individuals (data subjects) in a central position to self-manage personal data along with the risks associated with data processing. In contrast, the latter law operates by restricting the power of undertakings, especially those in a dominant position. Competition law is therefore paternalistic in the sense that it tackles power asymmetries through investigations, with little participation of the individual concerned. Conversely, data protection law has recently become characteristically individualistic as both consent and subject rights require a high level of individual engagement.

[20] Averitt and Lande (n 24) 713-4.
[21] Albertina Albors-Llorens, 'Competition and Consumer Law in the European Union: Evolution and Convergence' (2014) 33(1) Yearbook of European Law 163, 163-4.

## 3. The Convergence of EU Rules

The high-level commonalities of these three areas pave the way for the emerging convergence of EU law. This section provides an account of how these rules bleed into each other. To start with, the European Data Protection Supervisor is a pioneer in the exploration of EU law convergence. In its 2013-14 Strategy, the EDPS aimed to promote a data protection culture in which 'data protection principles find expression in all relevant areas of policy and law'.[22] In March 2014, the EDPS issued a preliminary opinion on several aspects of policy synergies[23], which has sparked an ongoing debate.[24] The EDPS argues that the three areas of law 'converge around a two-fold purpose - the promotion of the welfare of the individual and the facilitation of a single European market'.[25] In 2016, the EDPS opinion on enforcement of fundamental rights suggested that a holistic approach to implementing EU rules is feasible; the Digital Single Market Strategy represents a pivotal point of convergence to this end.[26]

The increasing interplay between these areas of law has also been noted in the literature. For instance, Albors-Llorens notes that consumer protection and competition law are 'theoretically and formally independent but linked by connections and mutual influences...which seem to have become even more pronounced in recent times'.[27] Costa-Cabral and Lynskey argue that data protection and competition law are members of the EU law family and have 'significant family ties'.[28] Helberger and others describe a complementary

[22] European Data Protection Supervisor, 'Towards Excellence in Data Protection' (Strategy 2013-2014, 22 January 2013) 8.
[23] EDPS (n 22) 26.
[24] For instance, see the Symposium on Data Protection and Competition Law by the Oxford Journal of International Data Privacy Law, available at <https://academic.oup.com/idpl/issue/8/3>accessed 24 May 2019.
[25] EDPS (n 22) 11.
[26] European Data Protection Supervisor, 'EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (Opinion 8/2016, 23 September 2016) 3.
[27] Albors-Llorens (n 42) 164.
[28] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11, 14.

relationship between consumer protection and data protection and propose an integrated 'data consumer law'.[29]

The remainder of this section describes three distinct forms of convergence between these EU rules: (1) privacy and data protection recognised in competition law analysis (2) consumer protection rules extending to 'free' services in exchange for data disclosure and (3) data protection right for competition and consumer welfare.

### *1) Competition Law as a Holistic Approach to Data Protection*

Traditionally, competition law focuses on the promotion of competition only. As Lynskey criticises, it hence falls short of capturing social harms caused by commercial practices, such as the implications for individual rights.[30] Recent theories of competition law take into account non-economic factors as well, notably including privacy and data protection. In parallel with the EU data protection regime, a structural approach to data protection has been widely advocated. As the EDPS suggests, privacy and data protection should be considered in the appraisal of companies' activities 'not as peripheral concerns but rather as central factors'.[31] In so doing, competition law would 'promote privacy-enhancing services (PETs)' and '[enable] greater consumer control over their own data'.[32] Notably, the EDPS contends that the refusal to grant access to personal information may 'justify a new concept of consumer harm for competition enforcement in the digital economy'.[33]

The German Federal Cartel Office (The Bundeskartellamt) has recently set a precedent for the convergence between data protection and competition law. Its investigation into Facebook's 'limitlessly amassing of user data' lead to the conclusion that Facebook is in a position of dominance and has abused its

[29] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427, 1427.
[30] Orla Lynskey, 'Regulating "Platform Power"' (LSE Law, Society and Economy Working Papers 1/2017, 11 April 2017) 1, 4.
[31] EDPS (n 22) 26.
[32] ibid.
[33] EDPS (n 22) 26.

dominant power in the social network market. Basically, Facebook collected user data from third-party websites and combined them with Facebook user accounts. Bundeskartellamt found that this data fusion constitutes an exploitative abuse and should have strictly subjected to the users' voluntary consent.[34] As Andreas Mundt, the President of Bundeskartellamt, put it, 'an obligatory tick on the box to agree to the company's terms of use is not an adequate basis for such intensive data processing'.[35]

Interestingly, the Bundeskartellamt's assessment is mostly established on the grounds of data protection rather than competition. In dealing with data protection issues, the Bundeskartellamt states that it is in close cooperation with the leading data protection authorities. To note, the Bundeskartellamt's novel approach is in clear contrast to the Commission's position, expressed in Facebook/WhatsApp merger, that 'privacy-related concerns...do not fall within the scope of EU competition law'.[36]

At the time of writing, the Bundeskartellamt's decision is not final as Facebook has appealed to the Düsseldorf Higher Regional Court.[37] Nevertheless, this German case, as the first precedent in the EU legal order, makes a good case for the convergence between data protection and competition law.

*2) Consumer Protection Rules Extending to the Digital Economy*

Consumer protection law traditionally confines itself to transactions in exchange for money. In the digital economy, however, many products and services are marketed as 'free' at the point of entry, but the price is paid, not in the form of money, but disclosure of personal information. The EDPS notes

[34] Bundeskartellamt, 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (Bundeskartellamt News, 7 February 2019) available at<https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>accessed 7 May 2019.
[35] ibid.
[36] Case No COMP/M.7217 *Facebook/WhatsApp*, p.29.
[37]'Facebook – Bundeskartellamt's Landmark Decision Blurs the Line between Data Protection and Competition Law (Linklaters, 28 February 2019) available at<https://www.linklaters.com/en/insights/publications/2019/april/facebook-bundeskartellamt-s-landmark-decision>accessed 7 May 2019.

that consumers are nudged to downloading and using the service 'without serious consideration'.[38] Since price is not paid in monetary terms, the costs and benefits of information disclosure are less acknowledged by consumers.

In the digital economy, data now operates 'as a currency, and sometimes the sole currency in exchange of online services'.[39] Many 'free' services also have their business model built upon a 'premium' version of the service, which requires monetary payment in a later phase.[40] More importantly, the level of data protection for the 'free version' is often reduced through a revised privacy policy and data protection law often falls short of restricting this contractual freedom. As Helberger and others put it, data protection law mainly addresses the fairness of data processing, rather than that of contracting.[41]

Against this backdrop, a modernisation of EU consumer protection law was initiated in 2015, which culminated in the proposal for a Digital Content Directive.[42] This Directive has been approved by the EU in April 2019 and, starting from 11 June 2019, the Member States have two years to transpose it into national law.[43]

This new consumer contract law in the EU converges with the GDPR in several ways. First, the Commission states that personal data is often seen as 'having a value comparable to money' in the digital economy.[44] The notion of 'counter-performance' was coined in the initial proposal to refer to the fact that many

[38] EDPS (n 22) 29.
[39] ibid 10.
[40] ibid 29.
[41] Helberger (n 50) 1427.
[42] European Commission, Proposal for a Directive of the European Parliament and of the Council on Certain Aspects concerning Contracts for the Supply of Digital Content, 9.12.2015, COM(2015) 634 final.
[43] Council of the European Union, 'EU Adopts New Rules on Sales Contracts for Goods and Digital Content' (Press Release, 15 April 2019) available at <https://www.consilium.europa.eu/en/press/press-releases/2019/04/15/eu-adopts-new-rules-on-sales-contracts-for-goods-and-digital-content/>accessed 24 May 2019. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services OJ L 136, 22.5.2019, p. 1–27, Art 24.
[44] Proposal for the Digital Content Directive, recital 13.

services marketed as 'free' are paid not by money, but by giving access to data. The notion itself was subject to severe criticism[45], and eventually abandoned by EU legislators. Despite this terminological issue, the Commission argues that a differentiation based on the nature of the counter-performance (money or data) would 'discriminate between different business models' and 'have an impact on the economic interests of consumers'.[46] Therefore, the Digital Content Directive extends to the digital economy by covering new forms of transactions not paid by money. Second, the Directive also recognises data protection principles as part of conformity to the supply of digital content or digital services. For instance, recital 48 states that the failure to comply with the GDPR principles *e.g.*, data minimisation, data protection by design and by default, and encryption, may be considered to constitute a lack of conformity.[47] Last, the Digital Content Directive is highly interconnected with the GDPR, and several schemes from both instruments are mutually complementary. Recital 39 of the Directive states that the GDPR right to erasure and the consumer's right to withdraw consent should apply fully in connection with the contracts covered by this Directive.[48] Further, the right to terminate a contract concerning the supply of digital content or digital services entails a right to data portability upon the termination of the contract.[49] As will be detailed in the next section, this new right is devised to complement Art 20 GDPR, and should hence be used together in practice.

### *3) Data Portability as a Means to Promote Competition and Consumer Welfare?*

In the A29WP's public consultation, numerous responses pointed to the fact that the interpretation of the GDPR right to data portability had been affected

[45] European Data Protection Supervisor, 'Opinion on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (Opinion 4/2017, 14 March 2017) 9-10. See also Axel Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2.
[46] ibid.
[47] Digital Content Directive, recital 48.
[48] Digital Content Directive, recital 39.
[49] Digital Content Directive, Art 16(4).

by ‘political discussions on data portability expressed in the ongoing debate’.[50] At that time, the porting of digital content was being reviewed by EU legislative bodies[51], and the Commission was proposing the porting of non-personal data as a building block of the European data economy[52]. As data portability is believed to have a role in facilitating switching and alleviating lock-in, attempts have been made, in both authorities’ opinions and scholarly literature, to align the GDPR right to data portability with the logic of competition or consumer protection.

First, data portability has a contested impact on competition. In the GDPR Impact Assessment, the Commission states that the possibility to move data between service providers would ‘increase competition in some sectors’ on the one hand, ‘make data protection an element in this competition’ on the other.[53] Similarly, the European Data Protection Supervisor (EDPS) argues that data portability would not only ‘prevent abuse of dominance, whether exclusionary or exploitative’ but also ‘empower consumers to take advantage of value-added services’.[54] As a result, data portability could ‘release synergies between competition law and data protection law’.[55]

This conception of data portability may have been ostensibly inspired by the practice of number portability, that is, that a user of a telephone service is allowed to change the service provider while retaining his or her telephone

[50] Application for Access to Documents - Ref GestDem No 2018/1669, Syndicat National de la Communication Directe.
[51] European Commission (n 63).
[52] European Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ‘Building A European Data Economy’, 10.1.2017, COM(2017) 9 final, p.4-5.
[53] European Commission, Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, SEC(2012) 72 final, p.106.
[54] EDPS (n 22) 36.
[55] ibid.

number(s).[56] The Universal Service Directive, in which number portability is prescribed in across the EU[57], aims to ensure the provision of services through effective competition and choice.[58] Recital 40 states that number portability is a 'key facilitator of consumer choice and effective competition in a competitive telecommunications environment'.[59] By analogy, both the Commission[60] and the EDPS[61] hence advocate that the right to data portability could, in a similar way, facilitate switching between processing service providers (data controllers). Further, increased mobility of data is likely to create a new market for personal data reuse, in which consumers direct their data towards third parties who offer value-added services.[62]

Based on these rationales, scholarly efforts have been made to align the GDPR right to data portability with the logic of competition. For instance, Engels argues that the right should be interpreted and implemented 'in a nuanced fashion to avoid the adverse effect on competition and innovation'.[63] Greaf and others suggest that the GDPR right's scope of application be restricted to the market of social networks to reduce the impact on other markets in which the degree of lock-in is relatively low.[64] This appears to be a sensible suggestion from a competition perspective but in tension with GDPR's general-purpose rationale. Further, while the need for data portability among

[56] Inge Graef, 'Mandating Portability and Interoperability in Online Social Networks' (2015) 39 Journal of Telecommunications Policy 502, 502. Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 European Law Review 793, 797.
[57] Art 30 of the Universal Service Directive states that 'end-users who so request should be able to retain their number(s) on the public telephone network independently of the organisation providing service'. See Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) OJ L 108, 24.4.2002, Art 30.
[58] Universal Service Directive, Art 1.
[59] Universal Service Directive, recital 40.
[60] European Commission (n 74) 28.
[61] EDPS (n 22) 15, 36.
[62] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 3. EDPS (n 22) 15.
[63] Barbara Engels, 'Data Portability Among Online Platforms' 5(2) Internet Policy Review 1, 10.
[64] Graef and others, 'Putting the Right to Data Portability into A Competition Law Perspective' (2013) Law Journal of the Higher School of Economics 53, 60-1.

social networks are particularly outstanding, we should not underestimate the emergent demand of data mobility in other sectors. Vanberg and Ünver contend that the GDPR right's adverse consequences, particularly for SMEs, can be alleviated by drawing lessons from EU competition law.[65] This alignment between data portability and competition is understandable given their historical connections illustrated in Chapter 1. That said, whether the GDPR right can legitimately promote competition is one thing, and whether it is instrumental in facilitating this goal is another.

Second, data portability has been framed as a remedy to lock-in, the practice that businesses adopt strategies or technical measures to make consumers or users more dependent on the service concerned. As a result, consumers who intend to switch to better, cheaper, and more privacy-friendly services in a certain market have to bear considerable switching costs. Indeed, data is playing an increasingly important role in the digital economy. Successful business models are all built heavily upon constant collection, analysis, and exchange of data. Whereas consumers are empowered to interact on social media and generate a large amount of data on web 2.0, businesses are now offered with cloud-based data processing and storage services that encourage data migration. As a result, data now constitutes a significant portion of the switching cost for both businesses and consumers. Shapiro and Varian contend that databases stand out as a source of consumer lock-in because a large volume of information is stored, manipulated, and communicated in unique, complicated, and opaque systems.[66] The degree of lock-in also 'tends to rise with time as more and more information comes to reside in the historical database'.[67] Veale contends that hyper-personalised services are increasingly

[65] 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 1, 1.
[66] Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Review Press 1998) 116.
[67] ibid 123.

valuable to individuals, but at the same time limiting access to a wider choice of service or suppliers.[68]

To free consumers or users from lock-in, data portability may only play a limited role. Shapiro and Varian note that the presence of lock-in results from a range of factors such as contractual commitments, durable purchases, brand-specific training, specialised suppliers, search costs, and loyalty programmes.[69] Burnham and others argue that the switching cost comprises procedural costs (concerning the loss of time and effort), financial costs (loss of financially quantifiable resources) and relational costs (psychological and emotional discomfort due to the loss of identity or the breaking of bonds).[70] Data portability may indeed be of help to alleviate lock-in when the exclusivity of data is the primary barrier to switching. It is of less relevance when the network effect (*e.g.*, the phenomenon where the increased number of people improves the value of a good or service[71]) is the major factor at play, or when consumers can alternatively 'multihome' on a number of equivalent services. As will be shown in Chapter 5, the technical challenge to interoperability, especially at the semantics level, also prevents consumers from enjoying a new service of equivalent quality, relevance, and convenience.

In line with this conception, it is believed that the GDPR right to data portability is, in essence, a consumer right. For instance, many Member States concerned that the right to data portability 'touches upon issues more properly regulated in competition and consumer protection law' and that 'coherence had to be maintained with those fields'.[72] The A29WP also implies in its Guidelines

[68] Michael Veale, 'Data Management and Use: Case Studies of Technologies and Governance' (The Royal Society, 2018) available at <https://www.thebritishacademy.ac.uk/sites/default/files/Data%20Governance%20-%20Case%20studies.pdf>accessed 13 October 2018.
[69] Shapiro and Varian (n 87) 117.
[70] Thomas Burnham, Judy Frels and Vijay Mahajan, 'Consumer Switching Costs: A Typology, Antecedents, and Consequences' (2003) 31(109) Journal of the Academy of Marketing Science 109, 109.
[71] *Facebook/WhatsApp* case (n 57) para 127.
[72] Application for Access to Documents - Ref GestDem No 2018/6570, Internal Report (Ares(2019)693034,11-12 July 2012), Internal Message (Ares(2019)693298, 13 March 2013), Internal Message (Ares(2019)693122, 9-11 April 2013).

that the right, which supports choice, control, and empowerment, 'provides consumer empowerment by preventing lock-in'.[73] In response to the A29WP's public consultation, numerous participants agree that the right is confined to a consumer-business relationship in the private sector because, as per Art 20(1) GDPR, it applies only to data processing legitimised on the grounds of consent or contract.[74]

## II. Data Portability Schemes in the EU: An Evolving Legal Landscape

Whereas the FFNPD facilitates the porting of data to which the GDPR is not applicable, the recently approved Digital Content Directive allows for the retrieval of non-personal data, thereby complementing the GDPR right to data portability. The last section compares these schemes to examine whether the GDPR right to data portability, irrespective of its objective, is instrumental in facilitating switching or alleviating lock-in.

### 1. The Free Flow of Non-Personal Data: Combating Vendor Lock-in

Similar to Art 20 GDPR, the FFNPD facilitates the porting of data between processing systems in a 'structured, commonly used and machine-readable' format.[75] This means that the FFNPD, aside from removing barriers to transborder data flows, addresses the issue of vendor lock-in directly. Recital 5-6 states that

Data mobility in the Union is also inhibited by private restrictions: legal, contractual and technical issues hindering or preventing users of data processing services from porting their data from one service provider to another or back to their own information technology (IT) systems, not least upon termination of their contract with a service provider… The combination of those obstacles has led to a lack of competition between cloud service

[73] A29WP (n 83) 3-5.
[74] Application for Access to Documents - Ref GestDem No 2018/1669. GDPR, Art 20(1), *cf.* Art 6.
[75] Regulation 2018/1807, Art 6(1)(a).

providers in the Union, to various vendor lock-in issues, and to a serious lack of data mobility.[76]

At the opposite of the GDPR, the FFNPD concerns the porting of non-personal data only, a controversial concept defined by reference to Art 4(1)(a) GDPR.[77] A Staff Working Document states that non-personal data primarily refers to 'commercial data and in particular machine-generated data, which are either non-personal in nature or have been anonymised'.[78]

As the FFNPD facilitates the flows of data to which the GDPR is not applicable, it pursues a purely economic objective of 'a competitive data economy'.[79] Recital 29 states that the ability to port data is 'a key factor in facilitating user choice and effective competition on markets for data processing services'.[80] Further, the Commission emphasised that data portability should 'not create an excessive burden on service providers or distort the market'.[81]

Following this competition-based rationale, the FFNPD framework adopts a self-regulatory approach to data portability, as opposed to the mandatory scheme in the GDPR. Whereas specific requirements for data portability are to be defined by market players, the Commission still plays a role in ensuring the involvement of all stakeholders, facilitate the codes of conduct at EU level (possibly through model contractual terms and conditions) and monitor their

[76] Regulation 2018/1807, recital 5-6.
[77] For instance, see Inge Graef, Raphael Gellert, Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (TILEC Discussion Paper No. 2018-029, 28 September 2018).
[78] European Commission, Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European data economy, SWD(2017) 2 final, p.4.
[79] Regulation 2018/1807, Art 6(1).
[80] Regulation 2018/1807, recital 29.
[81] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union, 13.9.2017, COM(2017) 495 final, p.2.

development and implementation within a clear timeframe.[82] Art 6(1) states that the Commission should facilitate the development of codes of conduct and best practices based on the principles of transparency, interoperability, and openness.[83] Recital 31 further lays down the key aspects of terms and conditions, such as the processes, the location of data backups, the data formats available, the required IT configuration, the minimum network bandwidth needed, the time for porting, and the guarantees for accessing data in the case of bankruptcy.[84] Notably, the codes of conduct should introduce certification schemes to facilitate the comparability of data processing products and services for professional users.[85]

### 2. The Supply of Digital Content: Tackling Consumer Lock-in

The Digital Content Directive creates a specific scheme for combating consumer lock-in. In the Staff Working Document, the Commission argues for the close link between the consumer right to terminate a contract, and the ability to retrieve data:

*The consequences of termination would include not only the return of the price corresponding to the unconsumed content, but also the possibility for consumers to retrieve data without inconvenience. This is an important feature of the termination right because otherwise lock-in effects could be created: this could make it disadvantageous for the consumer to exercise the right of termination and thereby reduce its effectiveness.*[86]

To tackle the lock-in, a consumer is now entitled, as per Art 16(4) of the Directive, to terminate the contract first, and then retrieve their digital content.[87] It should be noted that the final version of the Directive has diverged clearly from the Commission's initial position to create a set of legal rules parallel with

[82] Art 6(3) states that the Commission shall encourage service providers to complete the development of the codes of conduct by 29 November 2019 and to implement them effectively by 29 May 2020.
[83] Regulation 2018/1807, Art 6(1).
[84] Regulation 2018/1807, recital 31.
[85] Regulation 2018/1807, Art 6(1)(c).
[86] European Commission, Commission Staff Working Document Impact Assessment Accompanying the Document Proposals for Directives of the European Parliament and of the Council (1) on Certain Aspects Concerning Contracts for the Supply of Digital Content and (2) on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods, 9.12.2015, SWD(2015) 274 final, p.47.
[87] Digital Content Directive, Art 16(4).

the GDPR.[88] According to Art 13(2)(c) and 16(4) of the proposal, a consumer is entitled to 'all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content'.[89] The EDPS argued that Arts 13 and 16 of the proposal potentially overlaps with relevant articles of the GDPR, and might 'unintentionally lead to confusion regarding the regime applicable'.[90] It was suggested that the EU should 'avoid any new proposals that upset the careful balance negotiated by the EU legislator on data protection rules'. [91] In the final text of the Directive, suggestions from the EDPS have been accepted, with the Art 16(4) now brought in line with its GDPR counterpart. For instance, the consumer right to data portability in the Directive applies only to non-personal data, the scope of which is confined to those 'provided or created by the consumer when using the digital content or digital service'.[92] As per Art 16(4), consumers are entitled to retrieve digital content 'without hindrance from the trader...and in a commonly used and machine-readable format'.[93] By restricting the scope of portable content to non-personal data, the Digital Content Directive suggests the combined use of Art 20 GDPR to obtain a full copy of user-generated content/data.

To note, there exist several conditions for data retrieval that are not seen in the GDPR provisions. According to Art 16(3), the consumer's right to portability of non-personal data does not apply when

- The data has 'no utility outside the context of the digital content or digital service supplied by the trader';
- The data 'relates only to the consumer's activity when using the digital content or digital service supplied by the trader';
- The data has been 'aggregated with other data and cannot be disaggregated or only with disproportionate efforts'.

[88] Ruth Janal, 'Data Portability - A Tale of Two Concepts' (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 59
[89] The Commission's proposal for Digital Content Directive, Art 13(2)(c) and 16(4).
[90] EDPS (n 66) 3.
[91] ibid.
[92] Digital Content Directive, Art 16(4).
[93] ibid.

Ostensibly, these conditions would provide additional leeway for the trader not to provide data to consumers, thereby creating legal uncertainties on the possibility of obtaining all the data necessary for switching.

## 3. Revisiting the Right to Data Portability in the GDPR

To achieve the goals of facilitating switching, alleviating lock-in, and reusing personal data in a new IT environment, the data to be ported should not merely concern the individual, but also be useful or reusable in other IT environments. It is argued that the GDPR right, with unique objectives and pursuits, should neither be restricted by competition law rationale nor be overstretched to protect consumers from lock-in. From the outset, it appears to be a tool for multihoming rather than switching, allowing the data subject to port one copy of data for reuse. As explained previously, the scope of portable personal data concerned is, however, quite limited. The GDPR's intrinsic focus upon identification and identifiability prevents the inclusion of useful data and information other than personal data. Art 20(1) prescribes that the data portability right applies only to personal data 'provided by the data subject'.[94] This scope may be further narrowed down by the use of anonymisation, pseudonymisation and encryption in practice (as shown in Chapter 2) and protection of intellectual property rights, trade secrets and protection of databases (as will be explained in Chapter 4). With a limited scope of data concerned, it may fall short of achieving goals beyond data protection by itself.

To remedy this, the A29WP has attempted to ostensibly overstretch Art 20(1) beyond its literal meaning.[95] In its Guidelines, the data provided by the data subject is interpreted to include

- Data actively and knowingly provided by the data subject and
- Data provided by the data subject by virtue of the use of the service or the device (known as observed data)

By introducing a complementary scheme, the Digital Content Directive appears to have provided a solution to the dilemma once encountered by the

[94] GDPR, Art 20(1).
[95] A29WP (n 83) 9-10.

A29WP (now the European Data Protection Board). The new Digital Content Directive is devised in a way that well complements the GDPR, thereby suggesting the combined use of EU rules for consumer welfare. When enforced holistically, the consumer may potentially port all data necessary for switching. With the new Directive in place, it is now unnecessary to overstretch the GDPR provisions to tackle lock-in. It is suggested that the new EDPB should refine the A29WP Guidelines in accordance with recent developments in the EU when possible.

## Conclusion

The imperative of data protection is inherently associated with the free movement of personal data in the EU legal order. In this respect, this chapter examines the right to data portability from the perspective of data flows, looking at the right's potential to facilitate the data subject's economic well-being. Legal rules on consumer protection, data protection and competition are converging in the EU, and new schemes relating to data portability have been introduced to pursue goals other than data protection. Against this backdrop, this chapter navigates the right to data portability at the intersection of EU law and provides a detailed analysis of the right's essence, potential and externalities. Three major conclusions are made in this chapter.

First, the GDPR right to data portability cannot be solely justified on the grounds of the free flow of personal data, despite the proximity to this economic goal. Unlike the new schemes found in DCD and FFNPD, the GDPR right to data portability features a tenuous link to data protection and is somehow constrained by this feature. It can be gleaned from the divide between the GDPR and the FFNPD that whereas the porting of non-personal data facilitates a purely economic goal, the right to data portability cannot be legitimatised without resort to its data protection nature.

Second, the hybrid nature of individual control over personal data allows for the enhanced connection between data protection and other interrelated areas

of law. Through data portability, individual control now extends to the realm of consumer welfare, an overarching value that both consumer protection and competition law promote. Incrementally, the increasing access, transmission and reuse of personal data at the individual level may have a positive effect on data protection. In this sense, the right to data portability may be seen as pursuing both objectives in an unconventional order.

Third, the right to data portability would, together with the supply of digital content, plays a role in facilitating switching or alleviating lock-in. That said, this additional value does not prevent the GDPR right from being used for protection purposes. In sum, there are two different uses of the right to data portability, and the data subject may have to, at least in the short term, make a choice between data reuse and protection.

# Chapter 4 The Battle of Ownership: Balancing Personal Data Portability with Intellectual Property Rights, Trade Secrets, and the Protection of Databases

## Introduction

The previous chapter showed how the right to data portability interacts with consumer protection and competition law. Beyond data protection, this right may have an impact on the economic welfare of individuals as well. This chapter further looks at the right's interaction with intellectual property, trade secrets and database protection. These rules jointly provide data controllers with what this chapter calls 'information rights', the potential barriers to the implementation of the right to data portability.

The tension between data protection rights and information rights has been widely discussed in the narrative of data ownership. Both individuals and businesses claim 'ownership' of data on distinct legal grounds and the tension between the two have even been intensified in recent times. On the one hand, individuals are keen on regaining control over personal data and, with the new right to data portability, they are now entitled to have absolute control over a copy of their data. On the other, businesses have the incentive to prevent competitors and even users from extracting data from their database. To this end, they adopt various measures to maintain data exclusivity while at the same time seeking legal support.

Against this backdrop, this chapter examines whether and to what extent the right to data portability may come into conflict with rules on intellectual property rights, trade secrets and the protection of databases. This chapter comprises four parts. Part 1 provides an account of theories that conceptualise data in possessive or proprietary terms. Whereas *data as property* draws lessons from traditional principles of property law, *data ownership* carves out some room for exclusive control over data. Part 2 elucidates, from a practical perspective, the

growing tension between data protection and information rights. It is argued that the rights of both sides have been strengthened but neither of them allows for exclusive control over data. To address the potential conflict of rules, Part 3 examines the taxonomy-based approach on the premise that data protection rights generally apply to raw, personal and unintegrated data while information rights cover advanced, aggregated and machine-generated data. It will be revealed that existing taxonomies of data have their inherent limitations. As grey areas do persist, the conflict of rules is sometimes inevitable. Part 4 elucidates on the balancing principles found in both areas of law. A surprising schism exists between these principles when it comes to data portability: whereas the GDPR prioritise information rights over the right to data portability, the opposite is suggested in other instruments and case-law. To resolve this tension, this chapter examines the nature of the right to data portability in relation to data protection legislation and the right to data protection in the EU Charter of Fundamental Rights.

## I. The Theories of Data Ownership

Before addressing the tension between data protection and information rights, this section provides an account of two interrelated theories that have ostensibly inspired contemporary debates on data, ownership and property. Whereas *data as property* reflects upon the commodification of personal information in the digital economy, *data ownership* extends the bundle of proprietary rights (to possess, control, exclude, enjoy and deposit) to personal data.

### 1. Data as Property

The commodification of personal information (or 'datafication') in the digital age has invoked lively debates on the nature of data and our conception of (property) law. The idea of data as property has been extensively debated in legislative rhetoric, media reports and scholarly literature. It ostensibly derives

from the Lockean labour-desert theory.[1] In the Second Treatise of Government, Locke describes a state of nature in which goods are held in common and cannot be enjoyed in their natural state.[2] The individual converts goods into private property by his or her labour and, in so doing, adds value to the goods.[3] Translating this theory in digital context, Cohen describes that a person or entity 'owns' data generated by the labour and, as a result, has the right to 'prohibit or condition its use by others'.[4] This theory is not just favoured by private companies that process data but represents a radical approach to safeguarding an individual's informational privacy. Many scholars argue that 'propertisation' of data in full would put individuals in a position to make better privacy trade-offs and possibly acquire fairer compensation for information disclosure.[5]

Unlike traditional property such as food or land, data is not a scarce resource. Cohen points out that data is in essence 'profligate and casually escape from direct control'.[6] Similarly, Samuelson argues that 'while information privacy is a scarce commodity in cyberspace, information itself is not'.[7] In economic terms, the data governance is not concerned with 'how to allocate data given its scarcity', but 'how (or whether) to regulate its abundance'.[8]

---

[1] Justin Hughes, 'The Philosophy of Intellectual Property' (1988) 77 Georgetown Law Journal 287.
[2] John Locke, *Two Treatises of Government* (first published in 1690, CUP 1988) 265-8.
[3] ibid.
[4] Julie Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373, 1381.
[5] Kenneth Laudon, 'Markets and Privacy' (1996) 39(9) Communications of the ACM 92-100. Pamela Samuelson, 'Privacy as Intellectual Property' (1999) 52 Stanford Law Review 1125, 1132. Robert Bartlet, 'Developments in the Law--The Law of Cyberspace' (1999) 112 Harvard Law Review 1574, 1634-49. Richard Murphy, 'Property Rights in Personal Information: An Economic Defense of Privacy' (1996) 84 Georgetown Law Journal 2381, 2383. Lawrence Lessig, 'The Architecture of Privacy' (1999) 1 Vanderbilt Entertainment Law and Practice 56, 63-5.
[6] Cohen (n 4) 1382.
[7] Pamela Samuelson, 'Privacy as Intellectual Property?' (2000) 52(5) Stanford Law Review 1125, 1126.
[8] ibid.

Traditional property law requires that property must be freely alienable, that is, the capacity of a property (right) to be sold or otherwise transferred.[9] As Schwartz argues, free alienability of data refers to the ability of an individual to 'do whatever she wants with her personal information'.[10] This property-based conception may be in contrast to the fundamental rights to (data) privacy, according to which data '[should] not be divided into sticks in a bundle, surrendered, transferred or sold'.[11] As Renieris and Greenwood point out, the property law paradigm 'loses sight of intrinsic rights that may attach to our data...just because something is property-like does not mean that it is—or that it should be—subject to property law'.[12]

Similarly, Tene and Polonetsky are wary of using any property metaphor, arguing that it fails to 'capture the psychological and sociological nuance of the right to privacy'.[13] In its stead, they prefer the notion of benefit sharing, which ostensibly derives from the area of environmental law on biological diversity.[14] Tene and Polonetsky argue that if private companies intend to reuse personal data for other purposes, they should also 'share the wealth...with those individuals whose data they process'.[15] To note, the legal basis for benefit sharing in this context is hence not (quasi-)property rules but the doctrine of fairness.[16]

---

[9] Roger Smith, *Property Law* (Longman 1996) 1-2. See also Susan Rose-Ackerman, 'Inalienability and the Theory of Property Rights' (1985) 85 Columbia Law Review 931, 931.
[10] Paul Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2055, 2074.
[11] Elizabeth Renieris and Dazza Greenwood, 'Do We Really Want to "Sell" Ourselves? The Risks of a Property Law Paradigm for Personal Data Ownership' (HackylawyER, 23 September 2018) available at <https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa>accessed 27 May 2019.
[12] ibid.
[13] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11(5) Northwestern Journal of Technology and Intellectual Property 239, 269.
[14] For instance, see Elisa Morgera and Elsa Tsioumani, 'The Evolution of Benefit Sharing: Linking Biodiversity and Community Livelihoods' (2010) 15(2) Review of European Community and International Environmental Law 150.
[15] Tene and Polonetsky (n 13) 264.
[16] ibid.

A notion of 'quasi-property' has been discussed as a way to reconcile the interests of both parties. For instance, Balganesh defines quasi-property as property-like interests protected for 'simulating the functioning of property's exclusionary apparatus through a relational (liability-like) regime'.[17] The idea of quasi-property has been widely implemented in the area of trade secrets law. Samuelson contends that a number of 'default rules' in this area may be transferable to informational privacy protection.[18] For instance, if a licensor ('data owner') has provided data to another for a particular purpose, the data cannot be used by the licensee for purposes other than indicated without permission. Similarly, Schwartz proposes a hybrid-inalienability model, comprising restrictions on secondary data transfer and an opt-in default.[19] Basically, it allows an individual to trade personal data on the condition that he is entitled to 'further blocking transfers or uses by unaffiliated entities'.[20] That individual does not have to block actively since secondary data transfer is prohibited by default unless he gives consent to it.[21]

### 2. Data Ownership

Another strand of theories about data ownership inquires whether certain goods can be owned or not. This slightly different approach avoids the encounters with theoretical difficulties in propertising data but faces a number of challenges of its own.

In principle, private goods are characteristically rivalrous and excludable. Rivalry is a character that 'leads to the degradation of the quality or amount of good if used by another person'.[22] In simple terms, a rivalrous good can be 'used up' by one person and others cannot consume it anymore. Exclusivity is another attribute of private goods, meaning that the owner can use it

[17] Shyamkrishna Balganesh, 'Quasi-Property: Like, but not Quite Property' (2012) 160 University of Pennsylvania Law Review 1889, 1891.
[18] Samuelson (n 7) 1158-9.
[19] Schwartz (n 10) 2060.
[20] ibid 2098.
[21] ibid.
[22] David Weimer and Aidan Vining, *Policy Analysis: Concepts and Practice* (6th edn, Routledge 2017) 74-93.

exclusively, licence to a few others, and prevent others who have not paid for it from having access to it.

Data is not rivalrous because it can be, as Brin puts it, 'copied countless times at negligible cost'.[23] Data duplicability has been a copyright problem, as the copyright holder cannot effectively control replication. In the case of data ownership, however, it pleasingly allows multiple stakeholders to hold a copy of data of the same quality respectively. Data is also non-excludable because one set of data, such as group photos, may relate to a number of individuals. Urquhart casts light on the multi-dimensional nature of data ownership by arguing that data is 'often associated with more than one person and is hence relational in nature'.[24] Moreover, the Open Data Institute promotes an understanding of 'a wider network of relationship involved in data collection and use' as opposed to possessive pronouns.[25] Brin has a vivid description of the potential conflict data non-excludability may induce:

*A generalised principle of data ownership, if carried to its logical conclusions, would almost certainly produce a citizenry that spends half the next century in courtrooms, filing indignant injunctions to keep other people from sharing this or that snippet of knowledge without permission – in other words, a permanent entitlement programme for lawyers.*[26]

The theory of data ownership is fraught with limitations nonetheless. Cohen argues that it is 'a crabbed and barren way of measuring the importance of information that describes or reveals personality'.[27] As a concept, data ownership 'elides something vitally important and conceptually distinct about the interests that the term "privacy" denotes'.[28] Floridi attributes this discourse to a 'pre-digital' culture in which a metaphorical sphere of personal information

[23] David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Basic Books 1999) 95-6.
[24] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317, 326.
[25] Gillian Whitworth and others, 'The EU General Data Protection Regulation: Opportunities for Grocery Retail' (Open Data Institute Whitepaper, 4 December 2017) 2.
[26] Brin (n 23) 91.
[27] Cohen (n 4) 1378.
[28] ibid.

is advocated.[29] In this sphere, the access and usage of data 'ought to be fully controlled by its owner and hence kept private'.[30] In the digital age, however, private information is not kept secretly by each individual, but massively collected, aggregated and exchanged by commercial entities. As Tene and Buchner point out, the ownership of data for individuals is not, self-evident.[31] It bears little resemblance to the reality that private companies *de facto* collect, possess and control data to the exclusion of individuals concerned. As will be argued in Chapter 6, some user-centric technologies might make a case for individual ownership of data.

Despite some limitations, the theories examined above have somehow shaped recent law-making, public discussions and scholarly debates. Their influence is also evident, as will be shown in the next section, in the conception of data portability schemes.

## II. Owning Personal Data: The Contemporary Socio-legal Landscape in the EU

In practice, there are two ways in which commercial entities process data to the exclusion of others, what this Chapter calls 'data exclusivity'. First, technical measures are adopted to protect databases against third-party access, extraction and re-utilisation.

As illustrated in Chapter 2, anonymisation, pseudonymisation and encryption are playing an important role in keeping personal data secure. While not designed to construe data exclusivity, these measures may have an impact on third party access. More pertinently, the adoption of proprietary formats could place monetary or other restrictions on data reusability.[32] Data in those formats,

[29] Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2016) 92.
[30] ibid.
[31] Jerry Kang and Benedikt Buchner, 'Privacy in Atlantis' (2004) 18(1) Harvard Journal of Law and Technology 229, 238.
[32] Open Data Handbook: Glossary, available at <http://opendatahandbook.org/glossary/en>accessed 8 May 2019.

also known as ‘proprietary data’, can be processed only with the specific software owned by the commercial entity concerned.[33] The open data movement is indeed gaining momentum across the globe, promoting data openness, reusability and interoperability. However, the impact of proprietary formats and software is so significant that most business models ‘capitalise on the crucial discussions between proprietary and standardised formats’.[34] As Shapiro and Varian note, vendors are vulnerable to ‘new hardware or improved software to work with data...encoded in a specialised format’.[35] In addition, technical challenges to data interoperability also provide a natural shield against third-party access, as will be illustrated in Chapter 5.

Second, private contracts in the forms of Privacy/Data Policy and Terms of Use also contribute to data exclusivity. These standardised, non-negotiable and incomprehensible contracts one-sidedly determine how and to what extent businesses can collect, use, store and transfer user data, giving rise to a form of ‘digital feudalism’.[36] Indeed, the contract-based exclusivity is analogous to a feudal society in which the king capitalises on the abundance of land. Yen points out several features of cyberspace, such as consumer lock-in, contracts of adhesion and protection of intellectual property, amount to key components of a feudal society.[37] Meinratht and others point to the similarity of the massive collection of data to the enclosure (that is, a process of overtaking lands ‘to exploit the lands to the exclusion of others’).[38] Banta argues that standard contracts control our ‘digital assets’ and, as a result, create a *de facto* property system where ‘the powerful few create the terms of use of an asset for the many’.[39]

---

[33] ibid.
[34] ibid 123.
[35] Carl Shapiro, Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business School Press 1999) 122.
[36] Natalie Banta, ‘Property Interests in Digital Assets: The Rise of Digital Feudalism’ (2017) 38(3) Cardozo Law Review 1099, 1099.
[37] Alfred C. Yen, ‘Western Frontier or Feudal Society: Metaphors and Perceptions of Cyberspace’ (2002)17 Berkeley Technology Law Journal 1207, 1248-59.
[38] Sascha Meinratht, James Losey and Victor Pickard, ‘Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide’ (2011) 19 CommLaw Conspectus 423, 427.
[39] Banta (n 36) 1104.

Against this backdrop, this section examines the extent to which EU law responds to the exclusivity of data. It is noted that rules on intellectual property, trade secrets and the protection of databases jointly enhance technical and contractual exclusivity. In contrast, the EU data/consumer protection regimes impose restrictions on contractual freedom on the one hand, and remove technical barriers to data flows on the other.

## 1. Information Rights and Legal Exclusivity

There are a number of EU Directives that permit data controllers to hold data exclusively. For instance, trade secrets law protects 'know-how, business information and technological information' and holders may adopt measures to 'prevent, or obtain redress for, the unlawful acquisition, use or disclosure of their trade secrets'.[40] Copyright law covers creative databases and data therein; in either case, the author is entitled to prevent third parties from copying creative works without permission.[41] While some databases are not protected by copyright due to a lack of originality, they are nevertheless under *sui generis* protection in the EU. The database maker can 'prevent extraction and/or re-utilisation...of the contents of database'.[42] More recently, the framework of Free Flow of Non-Personal Data (FFNPD) further facilitates the portability of non-personal data for professional users, a new scheme that has been understood in possessive terms.

### *1) Data as Trade secrets*

The harmonisation of legal rules pertaining to trade secrets is a recent achievement in the EU. The Trade Secrets Directive was approved in June

[40] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-how and Business Information against their Unlawful Acquisition, Use and Disclosure (Trade Secrets Directive) OJ L 157, 15 June 2016, recital 14.
[41] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (InfoSoc Directive) OJ L 167, 22.6.2001, p. 10–19.
[42] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases (Database Directive) OJ L 77, 27 March 1996, Art 7.

2016 and, by 9 June 2018, the Member States are required to bring into force related domestic law.

Trade secrets protection prevents third parties from acquiring, using or disclosing trade secrets without permission. Notably, it is one of the legal grounds on which the data controller rejects individual access to personal data. When Max Schrems exercised his right of access against Facebook, pursuant to Irish Data Protection Acts 1998 and of 2003, the Data Access Request Team from Facebook claimed that the disclosure of some data would 'adversely affect trade secret or intellectual property of Facebook Ireland or its licensors'.[43]

Recital 2 of the Directive states that trade secrets cover 'a diverse range of information that extends beyond technical knowledge to commercial data, such as information on customers and suppliers, business plans and market research strategies'.[44] Art 2(1) sets out three criteria for trade secrets:[45]

1. The information is secret, meaning that it is not 'generally known among or readily accessible to persons within relevant circles'
2. The information has certain commercial value, either actual or potential, because it is secret
3. The information has been 'subject to reasonable steps under the circumstances to keep it secret'

It is argued in a report produced by Osborne Clarke that any sort of commercial or technical data may fall into the scope of trade secrets protection, according to the criteria mentioned above.[46] This is particularly true for personal data broadly defined by EU data protection law.[47] The Directive's Impact Assessment states that 'information kept as trade secret, such as a list of

[43] Letter from Facebook User Operations (Data Access Request Team) to Max Schrems, 28 September 2011, available at<http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf>accessed 8 May 2019.
[44] Trade Secrets Directive, recital 2.
[45] Trade Secrets Directive, Art 2(1).
[46] Osborne Clarke LLP, 'Legal Study on Ownership and Access to Data' (SMART number 2016/0085, 28 November 2016) 10.
[47] GDPR, Art 4(1). See also Nadezhda Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law' (2017) 10(1) Law, Innovation and Technology 40.

client/customers, internal datasets containing research data or other, may include personal data'.[48]

### *2) Data(base) as Copyrighted Works*

Personal data, if generated in a creative way, may be considered as copyright works.[49] The individual concerned is in oftentimes the author of the generated data but platforms often seek full permission to use the user-generated contents (UGC) as part of the contract. As Malgieri points out, popular platforms often explicitly recognise user rights subsisting on the contents, while 'requiring wide and free licence reuse, modify or economically profit from such [contents]'.[50]

Businesses may claim their own copyright that subsists on the database as a whole. According to the Database Directive, the acts of selecting and arranging data (database making) can be protected as copyrighted works.[51] Art 3(1) states that the databases have to reach a minimum standard of originality, amounting to 'the author's intellectual creation'.[52] With regard to the level of originality required, the Luxembourg jurisprudence has developed some contexts in recent years.[53] In *Football Dataco*, for instance, the Court of Justice of the European Union (CJEU) establishes that 'the author expresses his or her creative ability in an original manner by making free and creative choices, through the selection and arrangement of data which it contains'.[54] The

[48] Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) against their Unlawful Acquisition, Use and Disclosure, COM(2013) 813 final, p.254.
[49] Steven Hetcher, User-Generated Content and the Future of Copyright: Part One - Investiture of Ownership' (2008) 10 Vanderbilt Journal of Entertainment and Technology Law 863.
[50] Gianclaudio Malgieri, 'User-provided Personal Content' in the EU: Digital Currency between Data Protection and Intellectual Property' (2018) 32(1) International Review of Law, Computers and Technology 118, 123.
[51] Database Directive, Art 7.
[52] Database Directive, Art 3(1) and recital 15-16.
[53] Case C-5/08 *Infopaq International* [2009] ECR I-6569, paragraphs 35, 37 and 38; Case C-393/09 *Bezpečnostní softwarová asociace* [2010] ECR I-13971 paragraph 45; Joined Cases C-403/08 and C-429/08 *Football Association Premier League and Others* [2011] ECR I-9083, paragraph 97; and Case C-145/10 *Painer* [2011] ECR I-12533, paragraph 87.
[54] C-604/10 *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others* ECLI:EU:C:2012:115, para 38.

threshold of originality is not reached when 'the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom'.[55]

It should be pointed out that the database making nowadays involves less and less creative efforts. As the Osborne Clarke report notes, many databases are now compiled through automatic capture and collation of data, which may involve significant labour, but be not original enough for copyright protection. As the labour and skill 'do not express any originality in the selection and arrangement of data', modern database making is rarely likely to meet the standard of creativity.[56] Indeed, technological advances now enable the so-called 'brute force' approach, a trial-and-error method to obtain information such as password using automated software.[57] As a result, neither the selection nor the arrangement of contents of a database requires significant skill or judgment.[58]

Even if a creative database is protected by copyright law, it does not necessarily mean that the contents in that database are protected in the same manner. Art 3(2) of the Database Directive prescribes that copyright 'shall not extend to [the] contents and shall be without prejudice to any rights subsisting in those contents themselves'.[59] In *Football Dataco*, the CJEU holds that the Database Directive 'concerns the structure of the database, and not its content nor, therefore, the elements constituting its contents'.[60]

[55] ibid para 39. See also C-393/09 Bezpečnostní softwarová asociace - Svaz softwarové ochrany v Ministerstvo kultury [2010] ECR I-13971, paras 48-49. Joined Cases C-403/08 *Football Association Premier League Ltd and Others v QC Leisure and Others* and C-429/08 *Karen Murphy v Media Protection Services Ltd* [2011] ECR I-09083, paragraph 98.
[56] Osborne Clarke LLP (n 46) 13.
[57] ibid.
[58] ibid.
[59] Database Directive, Art 3(2).
[60] *Football Dataco* (n 54) para 30.

### *3) Protection of Database (sui generis right)*

In parallel with copyright, there exists a *sui generis* right in the EU for the database maker to prevent others from extracting or re-utilizing the database without permission.[61] Art 7(1) of the Database Protection Directive states that

The Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.[62]

Apparently, *sui generis* protection is subject to the proviso that the database maker has made 'a substantial investment' in the obtaining, verification and presentation of the content. The issue of how substantial investment needs to be remains contestable. Art 7(1) merely states that the investment is measured on a qualitative or a quantitative basis, or by a combination of both.[63] Another issue of what constitutes 'a substantial part of the content of the database' (the last two lines of Art 7(1)) is unclear. Art 7(5) states that 'insubstantial part of the content of the database' can be included in this context if the extraction or re-utilisation is 'in a repeated and systematic manner'.[64]

### *4) A New Property Right to Non-Personal Data?*

So far, EU rules on intellectual property rights, trade secrets and database protection has been examined. It is concluded that these rules do not provide for exclusive control over data for businesses. In view of this, there is a growing body of literature discussing new forms of property rights in the EU.[65] Notably, the framework of Non-Personal Data (FFNPD), as already illustrated in previous chapters, has been understood as assigning property rights to

[61] Database Directive, Art 7(1).
[62] ibid.
[63] ibid.
[64] Database Directive, Art 7(5).
[65] Josef Drexl, 'Designing Competitive Markets for Industrial Data: Between Propertisation and Access' (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 257. Wolfgang Kerber, 'Governance of Data: Exclusive Property vs. Access' (2016) 47 International Review of Intellectual Property and Competition Law 759.

professional users. The EU Regulation does not explicitly recognise property rights as such, but several legislative documents have alluded to this property-based perception. In a Staff Working Document, the Commission identifies several 'problem drivers', notably including the ownership of data, treatment of personal data and industrial data, access and reuse, among others.[66] In the Digital Market Strategy for Europe, the Commission explains that the FFNPD will 'address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business-to-consumer, machine-generated and machine-to-machine data'. [67] Kerber explains that the property 'does not fit the basic logic of digital economy' and would 'hamper data-driven innovation'.[68] In his view, the FFNPD framework is concerned with 'a new *sui generis* right on non-personal data'.[69]

Arguably, the FFNPD framework is not concerned with personal data. The notion of 'non-personal data' refers to a growing volume of data produced by machines and used in machine-to-machine communication and data rendered anonymous. Whereas the former does not entirely fall into the scope of the rules examined above, the latter is arguably outside the scope of the GDPR. Concerns have been raised that this definition of non-personal data does not adequately rule out data protection concerns. For instance, Greaf and others argue that the boundaries of personal data are 'too fluid to act as a regulatory anchor' and that division as such may lead to 'strategic behaviour of firms exploiting regulatory rivalry'.[70] In the main, it remains unclear how 'commercial

[66] European Commission, Staff Working Document Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, SWD(2015) 100 final, p. 61.
[67] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe, COM(2015) 192 final, p.15.
[68] Kerber (n 65) 761.
[69] ibid 760.
[70] Inge Graef, Raphaël Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (TILEC Discussion Paper DP 2018-028, September 2018) 1. See also Inge Graef and others, 'Feedback to the Commission's Proposal on A Framework for the Free Flow of Non-personal Data', available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106791>accessed 30 May 2019.

data', otherwise known as 'industrial data', 'proprietary data' or 'non-personal data', overlaps with personal data protected by the GDPR.

## 2. GDPR as a Property Regime?

GDPR is a set of new rules that is potentially in conflict with intellectual property rights, trade secrets, *sui generis* protection. Arguably, this regulation is also operated in parallel with the framework of the free flow of non-personal data. As a right-based scheme, the GDPR has been widely conceived as a (quasi-)property scheme. Purtova, for instance, defends the idea of data propertisation and explores how property rights in personal data have been acknowledged by EU law.[71] Victor notes that the GDPR gives expression to the fundamental right to data protection but can still be reframed as a property regime for protecting privacy.[72] Malgieri argues that European data protection law is built upon a 'relational, relative forbearance' that closely mirror the quasi-property model.[73]

Indeed, the GDPR features an increased level of individual empowerment. Consent is still at the centre of EU data protection law and has been prioritised and specified.[74] It is accompanied by a group of rights, allowing the data subject to access, rectify, erase, and transmit personal data.[75] Through these subject-centric schemes, the GDPR provides for individual control over the whole lifecycle of data, from the collection, storage, aggregation to analysis, erasure and transmission.

Whereas conventional rights are reactive to data processing that goes awry, the new right to data portability is in essence proactive, making a case for the exclusive control over *a copy of* personal data. The new right also allows the data subject to self-manage their personal data, including reusing it for their

[71] Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011)
[72] Jacob M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123(2) Yale Law Journal 266, 266.
[73] Malgieri (n 50) 9-10.
[74] GDPR, Art 7.
[75] GDPR, Arts 13-22.

own benefits. Potentially, this might put the data subject in the position of the controller to determine the purpose, method and harvesting of data processing![76]

To note, the right to data portability is concerned with only *one copy of* personal data, and the process of porting itself does not affect the processing of *the original copy* still held by the data controller. As recital 68 states, the right to data portability does not prejudice 'the right to erasure, and in particular not imply the erasure of personal data concerning the data subject'.[77] Greaf and others argue that the right to data portability does not amount to a right to exclude, even used in combination with the right to erasure.[78] Therefore, the right to data portability is operated on the assumption that data is non-rivalrous and hence can be duplicated multiple times for all stakeholders. It is devised to break down the exclusivity of personal data but does so by creating two parallel scenarios of data processing, management and reuse. The tension between data protection rights and information rights have therefore not been alleviated but complicated. It is true that all these rights, if exercised coherently and collaboratively, have the potential to enable property-like actions.[79] It is questionable, however, whether the GDPR provides for absolute control over personal data, as if assigning property rights to the data subject. As explained in Chapter 2, subject rights are highly atomised, and their enforcement far from coordinated. The joint use of GDPR rights is theoretically viable but possible in limited circumstances only.

[76] Recital 18 of the GDPR does entail a household exemption, which states that the GDPR does not apply to the processing of personal data by a natural person 'in the course of a purely personal or household activity' and thus 'with no connection to a professional or commercial activity'. With the rise of user-side technologies, however, there are blurring lines between personal and commercial use of personal data.
[77] GDPR, recital 68.
[78] Generally, Inge Greaf, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2017) Tilburg Law School Research Paper No. 2017/22, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875>accessed 18 October 2018.
[79] Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74, 84.

## III. Data Taxonomies as a Means to Avoid the Conflict of Rights

The previous section shows two groups of rules supporting or reducing the exclusivity of personal data. Neither of them allows for exclusive control over data for individuals or businesses. The tension between these rules has even been heightened in the evolving legal landscape. To strike a proper balance, this section first explores the validity of drawing lines between different categories of data to which information and data protection rights respectively apply.

### 1. Data Taxonomies: A Synopsis

The significance of taxonomies for data governance has been expressed in many regulatory frameworks. For instance, the World Economic Forum (WEF) contends that shared taxonomies drive meaningful progress and support a holistic approach to data governance.[80] A taxonomy of personal data is proposed as part of the multi-year project called Rethinking Personal Data, according to which personal data can be divided into three categories:[81]

1. volunteered data, data created and explicitly shared by individuals, such as social media profiles
2. observed data, data captured by recording the actions of individuals, such as location data
3. inferred data, data about individuals based on analysis of volunteered or observed information, such as credit scores.

In a similar vein, the Organisation for Economic Co-operation and Development (OECD) advocates 'application of different protective measure to different categories of personal data'.[82] In an Expert Roundtable, the Working Party on Security and Privacy in the Digital Economy discussed data

[80] World Economic Forum, 'A New Lens for Strengthening Trust' (Rethinking Personal Data Project, May 2014) 15-16.
[81] World Economic Forum, 'Personal Data: The Emergence of a New Asset Class' (Rethinking Personal Data Project, January 2011) 7.
[82] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para 3(a).

categorisations as a means to promote good governance, and proposed a slightly different taxonomy based on the origin of data:[83]

1. provided data, data originate from direct actions taken by an individual
2. observed data, data which have been observed by others and recorded in a digital format
3. derived data, data generated from other data, after which they become new data elements related to a particular individual
4. inferred data, *i.e.* results of the detection of correlations which are used to create behaviour predictions.

To note, 'derived data' stands out as an independent category in this category because, according to OECD experts, it is 'created in a mechanical fashion using simple reasoning and basic mathematics'.[84] In contrast, Inferred data can be seen as a product of 'probability-based analytic process', which is much more intricate than derived data.[85] The former data also has more recent origins, which date back to the 1980s when commercial entities were capable of developing credit scores.

A synthesis of taxonomies shown above is provided in the table below.[86] Based on this synthesis, the rest of the section reveals the implications of data taxonomies for the right to data portability as well as information rights.

[83] OECD Working Party on Security and Privacy in the Digital Economy, 'Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking' (DSTI/ICCP/REG(2014)3, 20 May 2014) 4-7.
[84] ibid 5.
[85] ibid.
[86] It should be noted that there are other taxonomies which are ostensibly irrelevant to the implementation of the right to data portability. OECD (n 83) 4.

| | Volunteered/(individually) provided data | Observed data | Derived and Inferred data |
|---|---|---|---|
| Origin | Direct actions taken by the individual | Observed and recorded by those other than the individual | Generated on the basis of other data |
| Awareness by individuals | Fully aware (of the data, but not the implications of data sharing) | Much less aware | Unaware ('black box') |
| Individual engagement | Yes | No | No |
| Legal status | Protected by GDPR | In dispute | Protected as Intellectual Property and/or Trade Secret |

Table 4.1 A synthesised version of data taxonomies

## 2. Data Taxonomies in the GDPR and A29WP Guidelines

As per Arts 4 GDPR, this Regulation apply to personal data as opposed to non-personal data (anonymous data).[87] Pursuant to Art 20(1), a further line is drawn between data provided by the data subject and data created by the data controller.[88] The WEF/OECD taxonomies show that data provided by the data subject originates from the direct actions taken by an individual. However, there exists a huge controversy over the scope of individually provided data in the wake of the guidelines from the Article 29 Working Party (A29WP). To give the new right to data portability 'its full value',[89] the A29WP adopts an unusually broad interpretation nonetheless. According to its Guidelines, portable data comprises two categories of data:[90]

- individually provided data, data actively and knowingly provided by the data subject, such as mailing address, user name and age
- observed data, data 'provided by' the data subject by virtue of the use of service or devise, such as search history, traffic data, location data and data generated by a wearable device (*e.g.* heartbeat)

[87] GDPR, Art 4(1) and recital 26.
[88] GDPR, Art 20(1).
[89] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 9.
[90] ibid 10.

Clearly, this interpretation is in contrast to the taxonomies shown above, which differentiate volunteered/provided data from observed data. This interpretation is arguably beyond the literal meaning of Art 20(1) GDPR as well. An analogy can be made to Art 13 GDPR, which is concerned with 'data collected from the data subject'.[91] Ostensibly, this article has a wider scope of data concerned than Art 20, potentially more suitable to cover observed data. Assuming that the two terms be interpreted differently, the A29WP Guidelines have ostensibly overstretched Art 20(1) on the scope of data covered. Evidently, this broader interpretation is in stark contrast with the abovementioned taxonomies in which observed data stands as an independent category.

Apart from this controversy, the A29WP Guidelines state that inferred and derived data, that is, data created 'on the basis of the data provided by the data subject', are generally outside the scope of data portability.[92] These advanced, aggregated and machine-generated data would, at the outset, fall into the scope of intellectual property rights, trade secrets and the protection of databases.

### 3. Data Taxonomies in Information Rights

Data taxonomies are also reflected in, to a lesser extent, the rules concerning intellectual property, trade secrets, and the *sui generis* database right. For instance, volunteered data normally falls into the scope of data protection, and if generated creatively, that of copyright. As the WEF contends, volunteered data often has a transactional nature, involves 'a deeper sense of unique ownership' by individuals, and has 'strong emotional ties' with them.[93]

Volunteered data is less likely to qualify as a trade secret. Much user-generated information on social media, for instance, is publicly available and not secret in nature. For data held secretly, *e.g.* personal files stored in a personal cloud, they are also unlikely to fall into the scope of protection as the

[91] GDPR, Art 13.
[92] A29WP (n 89) 10-11.
[93] WEF (n 80) 16-17.

storage service provider only provides infrastructure for data storage and is not, from a legal perspective, a data controller or right holder. Drexl further contends that the secrecy threshold excludes much information from being protected as trade secrets as it would be difficult to 'establish a link between the secrecy of information and its commercial value'.[94] This is because the usefulness of information is not preserved by its secrecy but revealed in correlations with other data.[95]

The legal status of observed data appears even murkier. The WEF contends that this type of data can be 'grouped along a continuum of how aware individuals are of its capture and use'.[96] There is also a general lack of awareness of 'how much observed data is being captured, how it is being used and the value that can be extracted in selling it'.[97] Where data is passively collected, as in the case of by WI-FI scanners, the sense of ownership 'tends to shift to the institution which originally captured it'.[98] Observed data is not provided by the individual but created by recording their use of a service or device, such as search history, traffic data and location data. Straightforward recordings are obviously unlikely to constitute 'an author's intellectual creation'.[99] Even if that be the case, several issues instantly arise as to the originality of observed data: who is the 'author' of observed data? To what extent is this data a product of creative freedom? At the time of writing, there still exists no relevant case-law at EU level.[100] It can be argued, however, that copyright is less likely to subsist on passively collected data, whose originality is highly in doubt. Observed data may qualify as trade secrets nevertheless. This type of data is often exclusively and secretly held by a commercial entity. It is generated to reveal insights about user behaviour, preference and mind-

[94] Drexl (n 65) 269.
[95] ibid.
[96] WEF (n 80) 16.
[97] ibid.
[98] ibid.
[99] Database Directive, recital 15.
[100] For instance, in *Promusicae*, the CJEU discussed IP address (a form of observed data) only as a means to identify copyright infringers. The legal nature of that data from a copyright perspective was not ascertained in that judgment. C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271.

sets, and clearly has a commercial value. Consumer profiles, for instance, are often kept secretly, compiled by businesses for advertising purposes, and protected by technical and organisational measures from unauthorised access.

There is no dispute that information rights subsist on inferred and derived data, the creation of which has, as the WEF puts it, 'a lesser degree of individual awareness'.[101] Companies often have 'stronger claims over these data based on their investment or intellectual property'.[102]

| | Intellectual property (copyright) | Trade secret | Sui generis protection |
|---|---|---|---|
| Volunteered data (individually provided) | No (for the commercial entity) | No | Not for the data (*i.e.* content of the database) |
| Observed data | Unlikely | Yes | |
| Inferred or derived data | Yes | Yes | |

Table 4.2 The applicability of information rights on each category of data

Based on the analysis above, it is concluded that data taxonomies are generally useful to indicate which legal regime is applicable. The lines drawn between are not clear-cut and grey areas exist where information and data protection rights may clash with each other. This is particularly the case when the A29WP takes a broad interpretation of Art 20 GDPR and when the new Digital Content Directive further allows for the retrieval of non-personal data by consumers.[103] Observed data is a particular category of data to which both groups of rules apply and potentially come into conflict. As data taxonomies do not prevent the conflict of rights, the next section examines the balancing rules found in both areas of law.

[101] WEF (n 80) 16-17.
[102] ibid.
[103] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects concerning Contracts for the Supply of Digital Content and Digital Services OJ L 136, 22.5.2019, p. 1–27, Art 16.

## IV. *Ad hoc* Balancing

As the taxonomy-based approach does not adequately accommodate the technical complexities of data as well as the interaction of diverse rights, principles for balancing the rights in conflict are therefore needed. It is noted that principles as such exist in the GDPR as well as the EU instruments on intellectual property rights, trade secrets, database protection and free flow of non-personal data. However, a surprising schism is noted between them when it comes to data portability.

### 1. The Principle of 'Not Adversely Affect'

As per Art 23(1)(i) GDPR, all subject rights are subject to restriction on the ground of safeguarding 'rights and freedoms of others'.[104] Art 20 echoes this general restriction, prescribing that the right to data portability 'shall not adversely affect the rights and freedoms of others'.[105] The scope of 'rights and freedoms' seems broad and open to interpretation. Recital 68 states that the right to data portability 'should be without prejudice to the rights and freedoms of other data subjects'.[106] This explanatory note ostensibly suggests that 'without prejudice to' is synonymous with 'not adversely affect', and that it is the other data subject's rights and freedoms that Art 20 should not interfere with.

The A29WP Guidelines add that 'trade secrets and intellectual property of data controllers' should also be considered in this context.[107] This guidance makes a reference to recital 63, which states that the right of access 'should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software'.[108] Contestable as it may be, this extension based on the recital of the right of access might be justified. Historically, this line of recital 65 was first added in the Albrecht report, in which Rapporteur Albrecht suggested the merger of Art

[104] GDPR, Art 23(1)(i).
[105] GDPR, Art 20(4).
[106] GDPR, recital 68.
[107] A29WP (n 89) 12.
[108] GDPR, recital 63.

15 (right of access) and Art 18 (right to data portability).[109] This proposition was then rejected and the rights of access and to data portability were deemed as freestanding rights. However, the explanation about the balancing with information rights had not reflected in the recital concerning the right to data portability.

Based on the rules examined above, it can be concluded that intellectual property rights and trade secrets override the rights of access and to data portability in general. The A29WP contends that the results of considering intellectual property rights and trade secrets should not 'be a refusal to provide all information to the data subject'.[110] Somewhat perplexing, it also argues that the right to data portability is not 'a right for an individual to misuse information...that would constitute a violation of intellectual property and trade secret'.[111] Provisionally, the A29WP seems to balance the two group of rules by permitting the subject access to commercial data on the one hand, and discouraging the misuse of data on the other. The line between data access and misuse is, however, far from clear. Recital 65 explicitly makes a reference to software, suggesting that subject access should not prejudice the copyright subsisting on the codes. It remains contestable, at the data level, how data access/portability may be balanced with intellectual property rights, trade secrets and the *sui generis* database right.

### 2. Data Protection Prevails?

In general, EU Directives on information rights prioritise data protection (legislation) when the two groups of rules are in conflict. For instance, the Information Society Directive, a general legal framework for copyright and related rights in the information society, states that copyright protection 'should

[109] Jan Philipp Albrecht, Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Albrecht Report), A7-0402/2013, 21.11.2013, p.201.
[110] A29WP (n 89) 12.
[111] ibid.

be without prejudice to ...legal provisions such as data protection'.[112] Trade Secrets Directive 'respects the fundamental rights...notably, the right to protection of personal data'.[113] Recital 35 states that this Directive 'should not affect the rights and obligations laid down in the Directive 95/46/EC (data protection), in particular the rights to access personal data...and to obtain the rectification, erasure, or blocking of data'.[114] In addition, Database Directive states that the *sui generis* right is 'without prejudice to existing rights over the content'.[115] Recital 45 adds that the provisions of this Directive are 'without prejudice to data protection legislation'.[116] Last, the Commission's Guidance on FFNPD acknowledges the case of mixed datasets, which comprise both personal data and non-personal data. Where these datasets are 'inextricably linked', the Commission establishes that the FFDPD shall not prejudice the GDPR implementation.[117] This is the case where the GDPR rights 'fully apply to the whole mixed datasets', and the Commission contends that personal data would 'represent only a small part of the dataset'.[118]

An integrated reading of these rules suggests, quite the opposite, that data protection (rights) overrides the rights of intellectual property, trade secrets and database protection. This reading has been partially confirmed by the CJEU jurisprudence. In *Promusicae*, the first case before the CJEU concerning the tension between data protection and intellectual property rights, the Court establishes that the Member States should not transpose intellectual property directives in a manner that conflicts with fundamental rights, notably including the right to data protection.[119] Further, in *Bonnier*, the CJEU holds that national courts have the authority to 'weigh the conflicting interests involved, and

[112] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society OJ L 167, 22.6.2001, p. 10–19, recital 60.
[113] Trade Secrets Directive, recital 34.
[114] Trade Secrets Directive, recital 35.
[115] Database Directive, recital 18.
[116] Database Directive, recital 48.
[117] European Commission, Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union, COM(2019) 250 final, p.9.
[118] ibid 10.
[119] *Promusicae* (n 100) para 70.

thereby ensures a fair balance between protection of intellectual property rights and that of data protection'.[120] In *Scarlet Extended*, the Court ruled that the filtering system concerned in that case was not operated on the basis of a fair balance between intellectual property rights, the freedom to conduct business, the freedom to receive or impart information and the right to protection of personal data.[121]

### 3. The Legal Status of the Right to Data Portability

Both EU Directives and CJEU case-law suggest that the rights of data subjects override the information rights of controllers. This is because, as Fuster contends, that data protection has been recognised as a fundamental right.[122] This contrasts with the A29WP Guidelines nonetheless, which suggest that intellectual property rights and trade secrets should not be 'adversely affected' by the data portability right. The schism between these approaches begs the question whether the right to data portability acquires the legal status of data protection when balanced with information rights. At fundamental-rights level, it is also worth exploring whether the right can be seen as giving expression to Art 8 of the EU Charter of Fundamental Rights.[123] As shown previously, EU rules on intellectual property rights, trade secrets and *sui generis* database right make references to 'Directive 95/46/EC', 'data protection legislation' and 'fundamental right to data protection' in an inconsistent manner. There appears to be a gap between these references and the new right to data portability.

Two critical facts should be noted in the first place. On the one hand, EU rules on intellectual property, trade secrets and the *sui generis* database right had all been enacted long before the GDPR entered into force in May 2018. On the other, the EU Charter of Fundamental Rights, which was introduced between

---

[120] C-461/10 *Bonnier Audio AB and Others v Perfect Communication Sweden AB* ECLI:EU:C:2012:219, 19 April 2012, paras 58-60.
[121] C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR I-11959, para 53.
[122] Gloria González Fuster, 'Balancing Intellectual Property Against Data Protection: A New Right's Wavering Weight' (2012) 14 IDP. Revista d'Internet, Dret i Política 34, 34.
[123] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, Art 8.

that period, has reconstructed the EU legal order by introducing a new right to data protection.

The GDPR is now the up-to-date legislation on data protection and should, as the EU instruments indicate, overall the rights of intellectual property, trade secrets and database as a principle. This does not necessarily mean that a specific component of this Regulation always prevails when balanced with those information rights. As explained earlier, the GDPR right to data portability may not always serve a protective purpose. Since this right was introduced after the Lisbon Treaty as well as the rules on intellectual property rights, trade secrets and *sui generis* database protection, the issue of whether the GDPR right can 'represent' data protection (legislation) should be assessed on a case-by-case basis. The GDPR right might acquire a superior legal status when, it is argued, the use is instantly associated with the objective of data protection. This can be achieved by using the right to channel personal data into user-centric technological systems for better management and protection, which will be introduced in Chapter 6.

At fundamental-rights level, it is not clear whether the GDPR right to data portability gives expression to the fundamental right to data protection. To start with, Art 8 of the EU Charter of Fundamental Rights (CFR) states that 'everyone has the right to the protection of personal data concerning him or her'.[124] The Explanatory Note identifies a number of the legal bases for this fundamental right, even including EU secondary law:[125]

- Art 286 of The Treaty establishing the European Community (now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union)
- Art 8 European Convention of Human Rights
- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Directive 95/46/EC

[124] EU Charter of Fundamental Rights, Art 8.
[125] Explanations relating to the Charter of Fundamental Rights, OJ 303/02, 14.12.2007, pp.17-35.

It is indeed a constitutional fallacy, as some scholars have pointed out[126], that the CFR is established by reference to the Directive 95/46/EC. Art 8(2) CFR nonetheless specifies the fundamental right with an apparent reference to Art 12 of that Directive. Two specific rights are articulated, *i.e.* the right of access and to rectification and, according to the Directive, the latter can be further divided into the rights to rectify, erase and block data.[127] The new right to data portability is fundamentally distinct from these rights, as explained in Chapter 2. Whereas the existing rights serve a *rectificatory* purpose, the new one is more prominently known for its *redistributive* effect – *i.e.* addressing the asymmetries of power by demolishing the exclusivity of personal data. Apart from that, the right to data portability also fits in a technology-mediated protection scheme, as will be explained in the last chapter.

Still, one can see the new GDPR right to data portability as an extension to the right to rectification. In particular, Art 20 is situated in a section of the GDPR entitled 'Erasure and Rectification', ostensibly suggesting a broad understanding of rectification. [128] The issue of whether the new right may serve a rectificatory purpose is ultimately an issue to be ascertained by the EU courts in a given case. It may suffice to say, however, that when used in tandem with user-centric technological systems (as will be illustrated in Chapter 6), the right to data portability stands a chance of being granted a status of fundamental rights.

## Conclusion

This chapter examines the growing tension between the right to data portability and information rights relating to intellectual property, trade secrets and the *sui generis* database protection. While individuals now enjoy enhanced rights such as data portability, businesses can still legitimately maintain a certain

[126] For instance, see Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 89-130.
[127] Data Protection Directive, Art 12(b).
[128] In this section, the right to data portability (art 20) sits next to that to rectification (art 16), to erasure (art 17) and to the restriction of processing (art 18). See GDPR, section 3.

level of data exclusivity, via a wide array of technical, contractual and legal measures.

A survey of those EU rules concerning information rights shows that they are subject to many limitations. Whereas copyright is unlikely to extend to databases that do not involve creativity, the *sui generis* protection of databases is subject to numerous contingent factors (*e.g.* the degree of investment and the portion of data concerned). Personal data may qualify as a trade secret, and the tension between the protection of personal data and that of trade secrets is particularly mounting. Further, the scope of data covered by the various rules is highly diverse. Whereas Trade Secrets Directive covers secret and commercially valuable information, copyright law protects original data and databases. The *sui generis* right applies to databases only, the content of which (*i.e.* data) varies from case to case. Therefore, these rules, even when applied together, do not provide for absolute control over data.

The tension between information rights and the right to data portability has even been heightened in an evolving landscape. The broad interpretation of GDPR provisions by the A29WP has blurred the lines between provided data and observed data. In addition, individuals are now allowed to access non-personal data via supplementary schemes detailed in the previous chapter. To reconcile the rights and interests involved, data taxonomies are adopted as a means of data governance. The boundaries of each category of data are, however, not clear-cut, and both data protection and information rights may simultaneously subsist on a certain dataset (*e.g.* observed data). In addition, the case of mixed datasets where personal and non-personal data are 'inextricably linked' poses challenges to the application of the GDPR and the FFNPD.

The principles for balancing rights in conflict do exist in both areas of law but they seemingly provide conflicting guidance. Whereas the GDPR stipulates that data portability should give way to information rights, EU Directives and

CJEU case-law suggest otherwise. This disparity begs the question whether the GDPR right may 'represent' data protection, or be granted the status of a fundamental right. This is indeed an issue for the EU Courts to decide. Still, it suffices to say that the right to data portability stands a chance of being granted a legal status of (the right to) data protection, if used together with user-centric systems to be introduced in the next chapter.

So far, the GDPR right to data portability has been examined through the lens of data protection (Chapter 2), consumer protection and competition (Chapter 3), and intellectual property rights, trade secrets and database protection (Chapter 4). From the outset, the GDPR right appears to be a game-changer in the current asymmetries of power and information. The legal analysis above shows that it is heavily fettered by various legal rules nonetheless. The operability of the right faces not only legal challenges, and Chapter 5 examines a range of technical difficulties that can also impede the right to data portability.

# Chapter 5 Facilitating Data Portability/Interoperability through Soft Law: Technical Specifications for Data Reusability and the Role of Data Protection Authorities

## Introduction

The previous Chapters examined various legal barriers to the implementation of the right to data portability. Further to this, the GDPR right also confronts technical hurdles of several types. While it is relatively easy to move certain datasets from one system to another, the datasets cannot readily adapt to a new processing system after transmission, unless some technical specifications are achieved. Both the GDPR and other EU instruments explicitly mandate or encourage the fulfilment of certain specifications as such, which cannot be adequately understood without recourse to the knowledge of data science.

This Chapter looks at the technical specifications required to enable seamless transmission of personal data while ensuring that data can be reliably re-used in a new system. It also looks at the role of soft law (*i.e.* guidelines from data protection authorities at EU and national levels) in facilitating the removal of technical barriers. The Chapter is divided into five parts. First, it introduces several pairs of concepts essential to ensure data portability but less familiar to the legal world. To ease the understanding of data portability, Part 2 builds upon these concepts and introduces a simplified conceptual model that consists of three layers of interoperability (transport, syntax and semantics). It should be acknowledged that the simplified model discussed draws heavily on the existing discussions and that this Chapter does not provide original contribution to the modelling of interoperability. Part 3-5 reconstructs the Guidelines from the Article 29 Working Party on the basis of the conceptual model introduced. Several legal issues in relation to each layer of interoperability are addressed, including the methods to deliver data portability,

the use of proprietary versus open formats, and the role of metadata in achieving interoperability.

## I. Key Concepts

Before introducing the conceptual model of data interoperability, this section explains several pairs of concepts that jointly underpin that model. These concepts include portability and interoperability, data and software portability, structured and unstructured data, proprietary and open formats, data and metadata, and syntax and semantics. As many of them are highly interrelated and sometimes interchangeably used, it is essential to discern their subtle differences.

### 1. Portability and Interoperability

Interoperability and portability are 'two sides of the same coin' that have been often referred to in parallel.[1] Interoperability refers to a broad range of interconnectivity issues between machines, human beings, and institutions.[2] In the context of machine-to-machine communication, interoperability is defined as 'the ability of two systems or components to exchange information and to (mutually) use the information that has been exchanged'.[3] Similarly,

[1] Kiranbir Kaur, Sandeep Sharma and Karanjeet Singh Kahlon, 'Interoperability and Portability Approaches in Inter-Connected Clouds: A Review' (2017) 50(4) ACM Computing Surveys Art 49, 3. Stefan Kolb and Guido Wirtz, 'Towards Application Portability in Platform as a Service', in *Proceedings of the IEEE 8th International Symposium on Service Oriented System Engineering* (IEEE 2014) 218; Fotis Gonidis, Iraklis Paraskakis, and Dimitri's Kourtesis, 'Addressing the Challenge of Application Portability in Cloud Platforms' (2012), in Proceedings of the 7th South-East European Doctoral Student Conference 565; Kostas Stravoskoufos and others, 'A Survey on Approaches for Interoperability and Portability of Cloud Computing Services' (2014) CLOSER 112; Magdalena Kostoska, Marjan Gusev, and Sasko Ristov, 'An Overview of Cloud Portability', in Octavian Fratu, Nicolae Militaru, Simona Halunga (eds.), *Future Access Enablers of Ubiquitous and Intelligent Infrastructures* (Springer 2015) 248–254; Grace A. Lewis, 'The Role of Standards in Cloud-computing Interoperability', in Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS 2013) 1652–1661; Elena Markoska, Ivan Chorbev, Sasko Ristov, and Marjan Gusev, 'Cloud Portability Standardization Overview', in *Proceedings of the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO 2015) 286–291; Eleni Kamateri and others, 'Cloud4SOA: A semantic-interoperability PaaS solution for multi-cloud platform management and portability', in *European Conference on Service-Oriented and Cloud Computing* (Springer-Verlag 2013) 64-78.

[2] John Palfrey and Urs Gasser, Interop: The Promise and Perils of Highly Interconnected Systems (Basic Books 2012) 37-58.

[3] International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Cloud Computing - Interoperability and Portability', (ISO/IEC

Palfrey and Gasser refer to interoperability as 'the ability to transfer and render useful data and other information across systems, applications or components'.[4] The European Committee for Interoperable Systems points out that after two interoperable systems interact, the data or software 'continues to reside on the same physical system' (without any physical migration).[5]

In contrast, portability is concerned with the physical moving of system components from one system to another, whether it be datasets, software or other components. It is important to note that data portability is not merely about moving data around, but the objective of reliably adapting data to a new environment. Chetal and others define portability as 'removing dependencies on the underlying environment'.[6] According to the International Organisation for Standardisation (ISO), data portability refers to the ability to 'move and suitably adapt data between systems, at low cost and with minimal disruption'.[7] These definitions seem to suggest that data portability is not a binary concept; it is nonsensical to ascertain whether a set of data is portable or not since every bit of data can be ported as long as enough resources are deployed. As the ISO puts it, data portability concerns 'the porting cost, the risk associated with the porting and how to control the costs and risks compared to the expected benefits'.[8] Similarly, Petcu and others contend that data portability is about '[minimisation of] human efforts in re-design, re-deployment of application, data and services'.[9]

---

19941:2017, 1st edn., 15 December 2017) 1; IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries 610 (IEEE 610-1990, 18 January 1991).

[4] Palfrey and Gasser (n 2) 5.

[5] European Committee for Interoperable Systems, '"Cloud Switching" and the Free Flow of Data – Portability and Interoperability of Software and Data across Cloud Services' (ECIS Special Paper, 27 June 2016), available at<http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability>accessed 13 November 2018.

[6] Aradhna Chetal and others, 'Interoperability and Portability' (Cloud Security Alliance Group 4, 22 August 2011) available at<https://cloudsecurityalliance.org/wp-content/uploads/2011/09/Domain-6.docx>accessed 25 November 2018.

[7] ISO/IEC 19941:2017 (n 3) 13.

[8] ibid vi.

[9] Dana Petcu and Athanasios Vasilakos, 'Portability in Clouds: Approaches and Research Opportunities' (2014) 15(3) Scalable Computing: Practice and Experience 251.

In a general sense, the two concepts have no direct interdependencies upon each other. As the ISO contends, interoperable systems do not necessarily support portability of software or data within them and a system enabling data portability is not always interoperable with other systems.[10] An important distinction derives from whether the data or software is physically moved or not. Whereas data portability demands the moving of data from one system to another, interoperability allows for the exchange of data without migration. The notion of data portability has been used in a broader sense and at times incorporate data interoperability, that is, the ability of reusing personal data without the need to migrate data physically between systems. In this sense, interoperability provides for an automated means to achieve data portability, allowing data to flow through designated interfaces of two interoperable systems. As will be explained later, this is an expensive and technically demanding means encouraged by law.

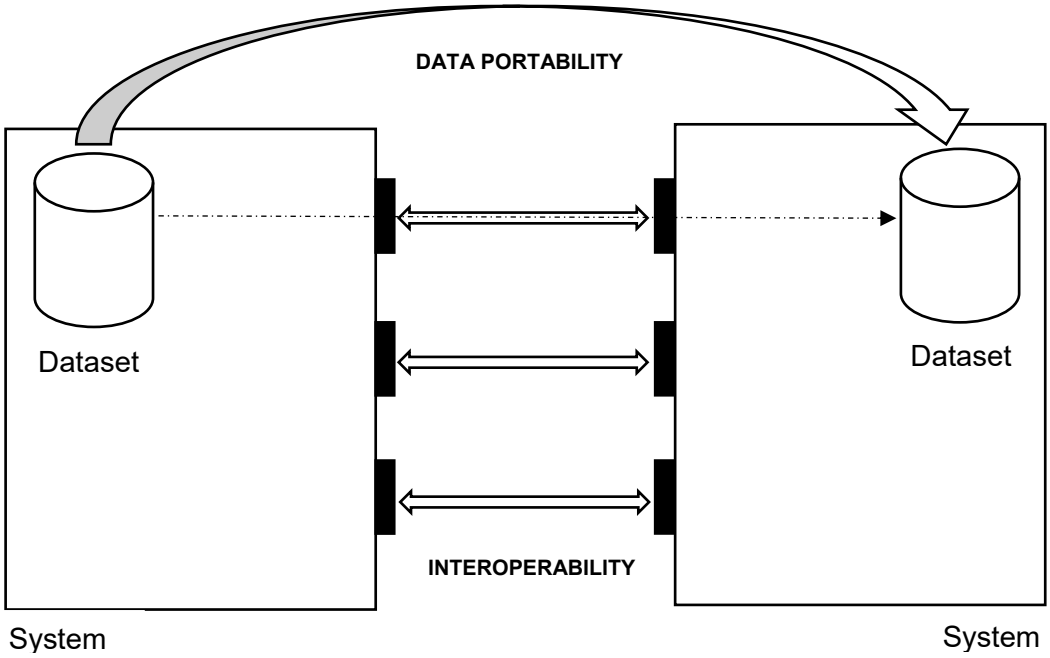


Diagram 5.1 An illustration of data portability and interoperability

[10] ISO/IEC 19941:2017 (n 3) 8.

## 2. Data and Software Portability

If data can be migrated from one system to another, so can software or applications designed to process data. Software portability represents an alternative solution to cross-system data re-use. Similarly, it is not a binary concept and implies a certain level of software adaptability. As the Cloud Security Alliance points out, certain software should well adapt to the new IT environment after migration, 'without having to be re-designed, re-coded or re-compiled'.[11]

The porting of software is particularly commendable when a large, complex dataset cannot be easily moved around. That said, this solution has its limitations. The ECIS points out that software portability is mostly affected by 'dependencies on other computing components such as middleware, software runtimes, operating systems, databases or hardware architecture'.[12] It is not commendable when the moving of software would take an overhaul of the operating system.

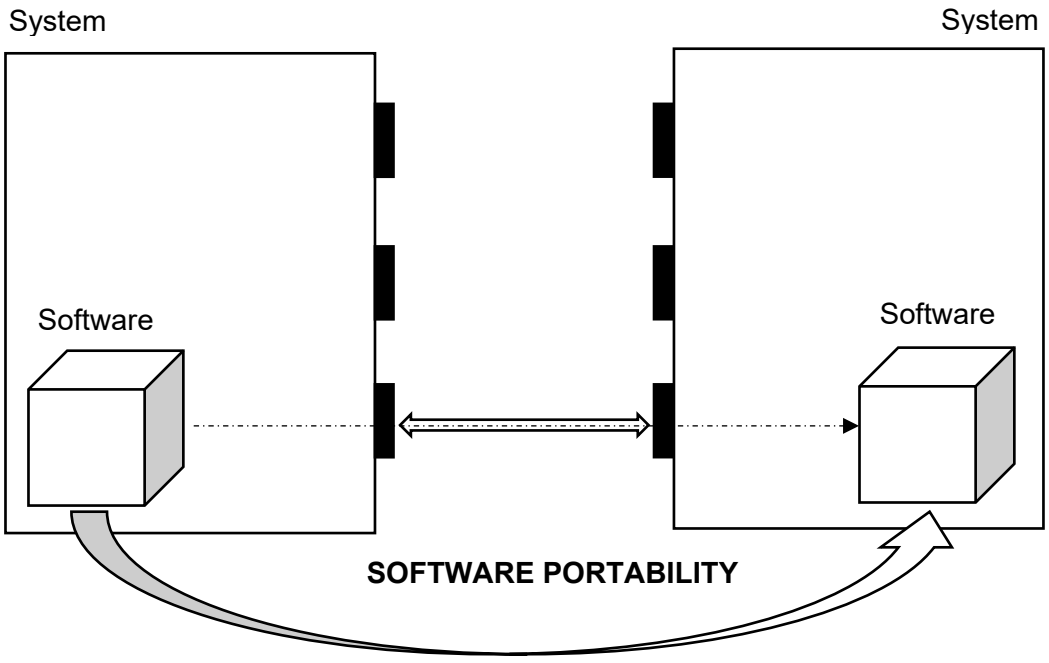


Diagram 5.2 An illustration of software portability

[11] Chetal and others (n 6) 9.
[12] ECIS (n 5).

### 3. Structured and Unstructured Data

The logic structure of data is a crucial factor to achieve data portability or interoperability. As the Open Data Handbook puts it, all data has some sort of structure, but not all of them are 'structured' data.[13] Data structure refers to 'the structural relation between elements, which is logically explicit to computer' (as opposed to human).[14] For example, tabular data expressed in a spreadsheet (*i.e.* data arranged in rows and columns) are often structured data, but there are exceptions.[15] Typical examples of unstructured data include the image, audio and video files.

### 4. Human- and Machine-readability

At the turn of the century, Berners-Lee and others noted that most of the web content is 'designed for humans to read, not for computer programs to manipulate meaningfully'.[16] To enhance machine intelligence, their ground-breaking project called the Semantic Web aims to create a web of information understandable by computers. Machine-readability pursues a logic completely distinct from human readability. As argued in Chapter 2, this distinction is the underlying basis for differentiating the right to data portability and of access in the GDPR.

Data structure is important because it determines a vital attribute of data, that is, machine-readability. As long as data is structurally represented, it can be automatically recognised, processed and re-used immediately after being transmitted to a new system. The Open Data Handbook asserts that 'machine-readable data must be structured data'.[17] In a similar vein, the Guidance from

[13] Open Data Handbook: Glossary, available at <http://opendatahandbook.org/glossary/en>accessed 5 December 2018.
[14] ibid.
[15] For example, tables in PDF format (without sufficient amount of metadata) are not structured data as the format concerned is not machine-readable.
[16] Tim Berners-Lee, James Hendler and Ora Lassila, 'The Semantic Web' (Scientific American, May 2001) available at <https://www.scientificamerican.com/article/the-semantic-web>accessed 30 November 2018.
[17] Open Data Handbook (n 13).

the UK's Information Commissioner's Office (ICO) states that 'if a format is structured, it is also machine-readable'.[18]

According to the Open Data Handbook, machine-readable format is defined as the format that 'can be automatically read and processed by a computer'.[19] The Public Sector Information Directive (PSI Directive) defines it as a file format 'structured in such a way that software applications can easily identify, recognise and extract specific data'.[20] Nonetheless, if a proprietary format limits automatic processing because data cannot be easily extracted from it, the Directive does not consider it as a machine-readable format.[21] Recital 21 states that machine-readable formats can be 'open or proprietary, and formal standards or not'.[22] In contrast, the World Wide Web Consortium (W3C) favours a definition that emphasises the independencies from proprietary software. It argues that a format is machine-readable only when computer programs can re-use data encoded in that format 'without the need for custom scripts to manipulate the content'.[23]

## 5. Proprietary and Open Formats

Not all data is created open. Some data in proprietary formats are not open in the sense that they cannot be reliably processed with free, open-source software. Typical examples include data in XLS or XLSX formats (owned by Microsoft).

Proprietary formats can be reliably read only with a certain proprietary software, which often places monetary or other restrictions on data re-use.[24] The Open Data Handbook notes the description of proprietary format is often 'confidential,

[18] Information Commissioner's Office, 'Guide to the General Data Protection Regulation' (ICO Data Protection, Version 1.0.248, 2 August 2018) 131.
[19] Open Data Handbook (n 13).
[20] 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 (PSI Directive) OJ L 175, 27.6.2013, art 1(2).
[21] PSI Directive, recital 21.
[22] ibid.
[23] Bernadette Hyland and others, 'Linked Data Glossary' (W3C Working Group, 27 June 2013) available at <https://www.w3.org/TR/ld-glossary>accessed 4 December 2018.
[24] Open Data Handbook (n 13).

unpublished and subject to arbitrary change'.[25] Users cannot use the data (unless they pay for the software), read or modify the source code (not open-source), and copy or resell the software (protected by intellectual property rights).[26] Because of these restrictions, the machine-readability of proprietary formats is contested.

Open formats are, in contrast, publicly available, set out in agreed standards, and overseen by a non-commercial expert body. By virtue of this openness, open formats are often used to pass information between different software programs. Common examples include Extensible Mark-up Language (XML), JavaScript Object Notation (JSON), Comma-Separated Values (CSV) and Abstract Syntax Notation One (ASN.1).

## 6. Data and Metadata

Metadata is known as 'data about data'; essentially, it is the information about a dataset. Metadata includes typically title and description, method of collection, author or publisher, area and time covered, licence, date and frequency of release etc. As a great contributor to the usefulness of data, metadata plays a crucial role in facilitating data discoverability, discernibility and reusability.

Metadata generally falls into two categories. Whereas the collection-level metadata describes how data is grouped in a data repository, file-level metadata gives contexts for a specific file within a dataset. The notion of granularity refers to the level of detail at which a certain dataset can be described by metadata. Low-level metadata is useful only to describe the collection process whereas highly granular metadata is needed for more detailed descriptions.

[25] ibid.
[26] ibid.

### 7. Syntax and Semantics

The distinction between syntax and semantics serves as the foundation of a layered model of interoperability, which this Chapter aims to introduce. This distinction initially emerged in the area of linguistics, in which syntax is concerned with the structure or order of a sentence, and semantics with the meaning of terms and expressions in that sentence.[27]

In the field of computer science, this differentiation between syntax and semantics can be traced back to several works of Claude E. Shannon, which look at ways to 'separate the technical problem of delivering a message from understanding what a message means'.[28] Veltman notes that the founders of computer science followed Shannon's approach and redefined the terms syntax and semantics in the second half of the 20th century.[29] According to them, computer syntax generally deals with the format, that is, the 'spelling of language components and the rules controlling how components are combined'. [30] Computer semantics is concerned with the meaning of a component.[31]

## II. Understanding Data Interoperability: A Layered Conceptual Model

Data interoperability is a technical achievement on the premise of several layers of specifications. Each layer is theoretically independent and, on each layer, there are multiple ways to achieve interoperability. On top of the concepts introduced above, this section presents a conceptual model of data interoperability (DIM) shown in the table below. It is primarily based on

[27] Kim H. Veltman, 'Syntactic and Semantic Interoperability: New Approaches to Knowledge and the Semantic Web' (2001) 7(1) New Review of Information Networking 159, 162.
[28] Claude Elwood Shannon, *The Mathematical Theory of Communication* (University of Illinois Press 1949).
[29] Veltman (n 26) 173.
[30] ibid.
[31] ibid.

European Interoperability Framework (EIF)[32], ISO/IEC Standards[33] as well as computer science literature. While these existing frameworks apply to distinct fields, sectors and IT environments, the basic technical specifications for cross-system data flows are much the same. DIM is a simplified model that comprises three layers: transport, syntax and semantics. It should be noted that, in other existing models, additional layers are built on top of them, *e.g.* business method layer, organisational layer, and human layer. Due to their limited relevance to the GDPR, these higher-level layers are omitted in the DIM.

| Layer | Objective | Object | Requirements | Level of development |
|---|---|---|---|---|
| Semantics | Interpretation of received data; Coordination of meaning of the content | Information | Common dictionaries and ontologies or schema mapping | Theoretically developed with practical implementation problems |
| Syntax | Automatic recognition and processing of the received data by the new system | data | Standardised exchange format or format converter | Fully developed |
| Transport | Secured data transfer between two systems; machine-to-machine communication | Signals | Data transfer protocols; infrastructure for protocols to operate | Fully developed |

Table 5.1 A conceptual model of data interoperability (DIM)

1. Transport Level

At the transport level, effective communications between systems are defined by a particular protocol, which describes the specific way data and other information are exchanged in a secured manner. Interfaces are often built within a system to support the connection and interaction with other systems.

Interoperability at the transport level can be achieved when participating systems use the same or compatible protocols. This is, however, not always

[32] European Commission, 'The New European Interoperability Framework' (ISA2, 9 May 2019) available at <https://ec.europa.eu/isa2/eif_en>accessed 9 May 2019.
[33] ISO/IEC 19941:2017 (n 3).

the case in reality. For instance, one system may adopt a Hypertext Transfer Protocol and another be built upon SSH File Transfer Protocol (SFTP). In that case, transport interoperability can also be fulfilled *pragmatically* by the adoption of adapters, such as 'Enterprise Service Bus'.[34]

### 2. Syntactic Level

In the DIM, syntax refers to the format used for the external exchange of data. A distinction should be made between the internal format used for data management and external format for transmission. Developers often have the freedom to choose the internal format, which is generally independent from external exchange.[35] When a certain dataset is to be transmitted to another system, it should be first encoded or encapsulated in a packaging format (syntax). Common examples of exchange format include Extensible Mark-up Language (XML), JavaScript Object Notation (JSON), Comma-Separated Values (CSV) and Abstract Syntax Notation One (ASN.1). Alternatively, data may be put into capsules such as Open Virtualisation Format (OVF) or ZIP.[36]

If participating systems use compatible syntaxes, the data can be immediately recognised, decoded and processed after transmission. As Berners-Lee notes, however, system designers independently develop their own syntaxes, adopt arbitrary structures to their documents, and provide no explanation on the structure used.[37] To address this fragmentation, syntax translators have been developed to map data encoded in different syntaxes.[38] The ISO notes that syntax mapping is 'generally possible and in some cases, can be performed

[34] ISO/IEC 19941:2017 (n 3) 12.
[35] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 17-8.
[36] International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Open Virtualization Format (OVF) Specification', (ISO/IEC 17203:2017, 2nd edn., September 2015); International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Document Container File -- Part 1: Core', (ISO/IEC 21320-1:2015, 1st edn., October 2015).
[37] Berners-Lee and others (n 16). See also Jon Bosak and Tim Bray, 'XML and the Second-Generation Web' (Scientific American, May 1999) available at <http://www.floppybunny.org/robin/web/virtualclassroom/xml/scientific_american_xml_web_may_1999.pdf>accessed 30 November 2018.
[38] ISO/IEC 19941:2017 (n 3) 12.

using widely available tools'.[39] The ease of mapping is considered an essential factor in evaluating data portability in qualitative terms.[40]

### 3. Semantics Level

Whereas syntactic interoperability provides for content-independent data exchange, semantic interoperability is further needed to understand the information conveyed reliably. As Kubicek and others put it, 'data becomes information on the semantics layer'.[41]

Interoperability at the semantics level is still a daunting task. The ECIS find it particularly complex when 'the destination system requires different content than the source system is capable of providing'.[42] Veltman argues that semantic interoperability is 'a quest to match equivalent fields in different systems', which often involves mapping, bridging, linking, creating crosswalks or walkthroughs.[43] Eventually, these efforts ensure that information is exchanged between systems on the basis of 'shared, pre-established and negotiated the meaning of terms and expressions'.[44] For example, we need to ensure that *football* and *soccer* are equivalent despite their cultural difference.

In history, there had been attempts to seek a single, universally valid meaning. These bold attempts were on the premise that the difficulties of semantics equivalency can be resolved by developing the international meaning of basic fields and elements. Most of them have floundered, however, simply because meaning is culture-dependent. As Veltman puts it, culture is concerned with 'exceptions to the rules and thus focuses on national, regional and local variants which are unique'.[45] Pragmatic tools have been developed for situations where ontologies used by participating systems (*i.e.* rules defining

[39] ibid 42.
[40] ibid vi.
[41] Herbert Kubicek, Ralf Cimander and Hans Jochen Scholl (eds), *Organisational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases* (Springer 2011) 89.
[42] ECIS (n 5).
[43] Veltman (n 26) 165
[44] ibid 167.
[45] ibid 168.

the relation between concepts) differ from each other. Notably, the use of metadata for schema mapping represents a major way to provide for semantic equivalency.[46] The ISO notes that the mapping process can be 'either straightforward or highly complex, depending on the nature of differences between semantic models'.[47]

The DIM provides a useful structure for understanding and assessing related GDPR provisions and A29WP Guidelines. The following three sections look at each layer of interoperability and the legal requirements associated with them. It is noted that, whereas the GDPR provisions primarily focus on the interoperability at the transport and syntactic levels, the A29WP Guidelines touch upon the issues of data semantics and metadata.

## III. Transport Interoperability and Alternative Ways to Deliver Data Portability

As illustrated above, interoperability at the transport level ensures that participating systems can effectively communicate with each other and that data be seamlessly exchanged through certain interfaces. Transport interoperability also provides for a fast, convenient and direct way of delivering data portability. In the GDPR Impact assessment, the Commission notes that data transfer is 'already possible through other interfaces, *e.g.* for third-party application developers or for exchanges with affiliated companies'.[48] Presumably, tools for compliance might be built upon existing interfaces. The Commission contends that the use of existing interfaces for complying with the

[46] ISO/IEC 19941:2017 (n 3) 12. See also International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Cloud computing - Overview and Vocabulary', (ISO/IEC 17788:2014, 1st edn., October 2014).
[47] ISO/IEC 19941:2017 (n 3) 46.
[48] European Commission, Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, SEC(2012) 72 final, p.106.

GDPR ‘may allow the development of portability functions very quickly...and the costs for implementation are minimal’.[49]

Indeed, interfaces built for system-to-system communication can be used to directly and seamlessly migrate data from system to system, without the need for individuals as the middle point of a transmission. However, the Commission seemed to be taking an over-optimistic view since special software or additional resources may be required to create a new interface or adapt existing ones.[50] This is the reason why Art 20(2) has been perceived as burdensome for data controllers, especially for SMEs.[51] This section looks at to what extent transport interoperability for data portability is mandated by the GDPR, and how much freedom data controllers have to choose a certain way to deliver data portability.

Art 20(2) GDPR states that the data subject may have the right to have their data ‘directly transmitted...where technically feasible’.[52] In connection to this, recital 68 states that there is no obligation for the data controller ‘to adopt or maintain processing systems which are technically compatible’.[53] It should be noted that compatibility is a technical term fundamentally distinct from technical feasibility. According to IEEE Glossary 610, compatibility is defined as ‘the ability of two or more systems or components to perform their required functions while sharing the same hardware or software environment’.[54] This requirement of same IT environments is absent in the context of interoperability, which is concerned only with system cooperation ‘despite differences in languages, interfaces and execution platform’.[55] The reference to compatibility in recital 68 is therefore not helpful to bring technical clarity, if not creating more confusion.

---

[49] ibid.
[50] ECIS (n 5).
[51] Peter Swire and Yianni Lagos, ‘Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique’ (2013) 72 Maryland Law Review 335, 369.
[52] GDPR, art 20(2).
[53] GDPR, Recital 68. See also A29WP (n 35) 16.
[54] IEEE (n 3).
[55] Peter Wegner, ‘Interoperability’ (1996) 28(1) ACM Computing Surveys 285, 285.

The A29WP is of the view that the criterion of technical feasibility relate to interoperability at both transport and syntactic levels. It means that the communication between participating systems is possible on the one hand, and that the receiving system is in a position to receive the incoming data on the other.[56] What may be gleaned from these guidelines is that interoperability at the transport level is not a legal mandate. The GDPR requires only a more realistic way of achieving data portability, that is, with the data subject in the middle of a transmission. The direct transmission between interoperable systems is a goal to be pursued.

Indeed, there is more than one method to achieve data portability. Apart from transport interoperability, a data subject may download one copy of the personal data first and then pass this on to another service provider she prefers. When a large, complex database is involved, data portability may be fulfilled by moving the storage media, such as a disk.[57] The A29WP suggests a number of methods to achieve data portability in its Guidelines, including[58]

- Secured messaging
- SSH File Transfer Protocol
- WebAPI
- WebPortal

| | Temporary storage required | Standardised | Adaptability | Use Case |
|---|---|---|---|---|
| Manual transmission | Yes | Yes | High | Data backup |
| Automatic transmission | No | Yes | High | Data migration |
| API-based access | No | No | Low | Data (real-time) analysis |

Table 5.2 Methods to achieve data portability

[56] A29WP (n 35) 15-6.
[57] ibid 7.
[58] A29WP (n 35) 16.

In the main, the suggested methods can be put into three categories and, as shown in the table above, each category has its advantages and disadvantages. Data exports represent an old-fashioned way of achieving data portability. It requires that the data be stored temporarily prior to the download, thereby requiring additional resources. Data portability can be also be delivered using protocols such as SFTP, which is particularly suitable for start-ups without legacy problems.

The Application Programming Interface (API) is an excellent way to deliver data portability and has been suggested for information society services.[59] The A29WP argues that the API-based solutions 'facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests'.[60] The Open Data Handbook states that API allows for 'the reading of data directly on the web, and (re-)use without downloading the whole dataset, therefore saving bandwidth and ensure data quality (*e.g.* up to date)'.[61] As this approach requires the data controller to program a specific interface for compliance, it is often technically and financially burdensome.

Apparently, there exists no one-size-fits-all solution. Depending upon what the data controller is technically capable of, and what the data subject needs data for, the optimal solution may be different. As Wang and Shah suggest, each category of methods shown above may be aligned with specific use cases (*e.g.* data archive, data migration and data analysis).[62] The A29WP suggests that data controllers should 'explore and assess two different and complementary paths' to achieve transport interoperability:

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
- an automated tool that allows extraction of relevant data.

[59] A29WP (n 35) 15.
[60] ibid.
[61] Open Data Handbook (n 13).
[62] Yunfan Wang and Anuj Shah, 'Supporting Data Portability in the Cloud under the GDPR' (2017) available at <https://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf>accessed 28 November 2018.

Among those, the A29WP seems particularly in favour of the second approach, arguing that it keeps the data obtained relevant, allows for data synchronisation, and is preferable in cases when large, complex datasets are involved.[63] From a data protection perspective, this approach also 'minimises privacy risks on the part of the initial controller' on the one hand, and 'ensures compliance for the new controller' on the other.[64]

In sum, it is suggested that proportionality and technology neutrality should be duly respected in this respect to ensure a certain leeway for controllers to find their optimal method(s). Further, the efficiency and costs of each method should be taken into account to avoid excessive burdens on data controllers.

## IV. Syntactic Interoperability: Mind the Gap between Common and Proprietary Formats

Syntactic interoperability is concerned with the data format for external transmission. The syntaxes used should be compatible so that data can be reliably recognised, decoded and processed by the new system. Otherwise, the data transmitted would be meaningless.

The issue of whether syntactic interoperability is required by the GDPR is contestable. Art 20(1) GDPR prescribes that personal data should be provided in a 'structured', 'commonly used' and 'machine-readable' format.[65] Further, recital 68 adds the 'interoperable' format, which is not seen in Art 20. The recital explains that data controllers should be 'encouraged to develop interoperable formats that enable data portability'.[66] This seems to suggest that the GDPR facilitates, rather than mandates, interoperability at the syntactic level. This view is supported by the A29WP Guidelines, which states

[63] A29WP (n 35) 16.
[64] ibid.
[65] GDPR, art 20(1).
[66] GDPR, recital 68.

that the terms ‘structured’, ‘commonly used’ and ‘machine-readable’ are ‘minimal requirements that should facilitate the interoperability of the data format’. [67] In other words, these format requirements in Art 20(1) are ‘specifications for the means, whereas interoperability is the desired outcome’.[68]

Elsewhere in the A29WP Guidelines, however, there seems to exist conflicting guidance. In interpreting the GDPR requirement that the data controller should supply personal data ‘without hindrance’, the A29WP argues that such hindrance ‘can be characterised as...technical obstacles placed by data controller… [and] could be lack of interoperability or access to a data format or API’. [69] Therefore, a lack of interoperability at the syntactic level might be impermissible as a form of hindrance.

Further, the A29WP appears to advocate a ‘unilateral’ conception of syntactic interoperability. Its Guidelines state that the sending controller is obliged to transmit personal data in an ‘interoperable format’, but this ‘does not place obligations on other data controllers to support these formats’.[70] In contrast to this conception, interoperability is inherently pragmatic, context-dependent and two-sided. The issue of whether the exchange format used by one system is interoperable should be assessed on a case-by-case basis.

It is noted that the GDPR provisions are vague on this point, and the A29WP Guidelines provide inconsistent and sometimes even conflicting guidance. From the outset, the interoperability at the syntactic level is not mandated at all. That said, one may argue that syntactic interoperability is *ensured* by the use of commonly used syntaxes. Chances are that these syntaxes are, or can be rendered by the use of adapters, compatible with each other. Presumably, it would not be difficult to convert one common format into another common

[67] A29WP (n 35) 17.
[68] ibid.
[69] ibid 15.
[70] ibid.

one. Further to this, the A29WP seems to have overstretched the GDPR provisions again by pointing to the use of open formats. The Guidelines state that controllers should 'provide personal data using...open formats (*e.g.* XML, JSON, CSV)' when no formats are in common use for a given context.[71] There surely exists a gap between commonly used formats and open formats. For example, Microsoft's DOC and XLS are extensively used in many sectors but proprietary in nature.

This advocacy of open formats is ostensibly influenced by the pursuit of interoperability in the public sector. For instance, the A29WP Guidelines suggests that lessons may be learnt from the EIF, designed for the delivery of public services. This framework indeed entails a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.[72] Further, the PSI Directive is built mainly upon open data principles. Art 5 states that public sector bodies should 'make documents available through open and machine-readable formats'.[73] Recital 21 adds that 'Member States should where appropriate encourage the use of open, machine-readable formats'.[74]

In contrast, the GDPR right to data portability is more likely to be used in the private sector where proprietary formats are the norm and open formats the exception. In this context, path dependency runs the risks of ruling out the use of proprietary formats, which is actually permitted by the GDPR. Efforts should be made to ensure that this path-dependent approach does not contravene principles such as proportionality and technology neutrality.

## V. Semantic Interoperability: The Myths about Metadata

The GDPR provisions are virtually silent on interoperability at the semantics level. To fill this gap, the A29WP Guidelines touch upon the issue of semantic

[71] ibid 18.
[72] ibid.
[73] Directive 2013/37/EU, Recital 20.
[74] Directive 2013/37/EU, Recital 21.

interoperability. For instance, it suggests a multi-stakeholder approach calling for collaboration with industry stakeholders and trade associations on a common set of interoperable standards and formats.[75] As noted above, experiences in the public sector are considered as a source of transferable elements, including vocabularies, concepts, and standards necessary for semantics equivalency. In this respect, the Interoperability unit of DG Informatics of the European Commission (DIGIT.D2), which is now responsible for the revision of EIF, has responded A29WP with a study on GDPR data portability. The report suggests that several core vocabulary specifications developed under the ISA2 programme, and Core Person Vocabulary in particular, are 'simplified, reusable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion'.[76] The study concludes that these vocabularies would provide a solution for interoperability and are potential enablers for the GDPR right to data portability.[77]

In addition, the A29WP acknowledges the importance of metadata in describing the meaning of personal data exchanged. The Guidelines state that 'data controllers should provide…useful metadata at the best possible level of granularity, while maintaining a high level of abstraction'.[78] This guidance, again, largely mirrors recital 20 of the PSI Directive.[79] Interestingly, the A29WP requires the provision of metadata but barely address the issue of metadata interoperability. The latter issue is critical because metadata, even provided in full, is virtually meaningless if unusable in a new IT environment. In contrast, recital 20 of the PSI Directive prescribes that metadata should be provided in a format that 'ensure interoperability, *e.g.* processing them in a way consistent with the principles governing the compatibility and usability requirements for

[75] A29WP (n 35) 18.
[76] Directorate-General for Informatics, 'GDPR Data Portability and Core Vocabularies' (ISA2 Programme, November 2018) 10.
[77] ibid 15-16.
[78] A29WP (n 35) 17.
[79] PSI Directive, recital 20.

spatial information'.[80] Similarly, the EIF requires that metadata should be machine-readable and in non-proprietary formats.[81] It should include 'a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available'. Further, the use of common vocabularies for expressing metadata is suggested.[82]

Further, the legitimacy of requiring the data controller to provide metadata seems questionable as well. On the one hand, it remains unclear whether metadata is to be provided on the ground that it falls into the scope of Art 20(1) or that, as the A29WP contends, it supports the objective of personal data re-use.[83] On the other, the provision of metadata would constitute a breach of trade secrets, as explained in the last Chapter. The A29WP argues that metadata should be provided 'without revealing trade secrets' but leaves the balancing of values mostly unaddressed.

As shown previously, the A29WP Guidelines provisionally overstretch the scope of portable data to entail observed data (*e.g.* metadata).[84] In contrast, the new Digital Content Directive now allows the consumer to obtain any content created when using the digital content or digital service, potentially including metadata as well.[85] In comparison, the Directive appears more suitable basis than the GDPR to provide the basis for supply of metadata since it entails rules for balancing metadata access and the rights and interests of traders. As per Art 16(4) of that Directive, the consumer right to access digital content does not apply when the digital content

- has no utility outside the context of the digital content or digital service supplied by the trader;
- only relates to the consumer's activity when using the digital content or digital service supplied by the trader;

[80] ibid.
[81] European Commission (n 32) 39.
[82] ibid.
[83] A29WP (n 35) 5, 18.
[84] ibid 9-10.
[85] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services OJ L 136, 22.5.2019, p. 1–27, art 16(4).

- has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts;

Indeed, these limitations might be used as an excuse not to provide metadata. It is argued that they would also play a role in reducing the risks of a breach of trade secrets and provide a solution for data subjects (also in the role of consumer) to access metadata legitimately. The European Data Protection Board (EDPB), now in the role of Article 29 Working Party, should refine the guidelines so that metadata is to be provided on the basis of the Digital Content Directive.

There are in the main two contrasting paths to semantic interoperability. On the one hand, there have been attempts, in both public and private sectors, to promote common standards as a means to achieve interoperability. The W3C has been a key advocate of open, common standards, suggesting a web of (linked) data known as the Semantic Web, originally coined by the wen inventor Sir Tim Berners-Lee among others.[86] At public sector, the European Commission has been facilitating standardisation for years. In the ICT Standardisation Priorities, for instance, the Commission sees common, open standards as the means to achieve interoperability and portability, hence indicating the financial support for the development and use of ICT standards. [87] Also in the ICT Standardisation Rolling Plan 2019, the Commission echoes the need for ICT standards to improve interoperability, data protection and portability of cloud services.[88] On the other hand, the stakeholders in the private sector, bearing in mind the difficulties in standardisation, favours pragmatic solution such as placing reliance on adapters as evidenced in the DTP White Paper.

[86] Natasha Noy and others, 'Semantic Integration & Interoperability Using RDF and OWL' (W3C Blog, 3 November 2005) https://www.w3.org/2001/sw/BestPractices/OEP/SemInt/
[87] ibid 26.
[88] European Commission, 'ICT Standardisation Priorities for the Digital Single Market', COM(2016) 176 final, p.6

At semantic level, the GDPR provisions are almost silent on the specifications that ensure data portability. The A29WP Guidelines are also ambiguous on this point, rendering interoperability as a goal to be achieved - and stopped at the establishments originally for the public sector only. The Guidelines have not explicitly suggested any of these two contrasting paths. Rather, it merely suggests that there has been in the European Interoperability Framework several sets of established concepts, principles and vocabularies that can be drawn on to implement the right to data portability.[89] As the connection as such has been made, it is argued that the experiences in the public sector may have an impact on the interpretation of legal provisions relating to data portability and interoperability.

It should be noted that standardisation is viewed as fundamental to interoperability under the European Interoperability Framework.[90] The EU administrations have been recommended to select, compare and integrate standards from various authorities, and to engage in the process of standardisation where there are not suitable standards.[91] At semantic level, interoperability is often achieved through agreements on standards and specifications.[92] Notably, the EIF explicitly endorses the standardisation approach and calls for agreements on reference data, controlled vocabularies, and reusable data structures/models etc.[93] The connection to the W3C's work is evident when the Commission recommends Linked Data Technologies as the innovative ways of achieving semantic interoperability.[94] Despite the diversity of linguistics, culture, law and administration in the Member States, the EIF concludes with standardisation efforts as the primary way, if not the only, to ensure the free movement of data and data portability among Member States.[95] It has to be noted that the EIF originally applies only to the public

[89] A29WP (n 35) 18.
[90] New European Interoperability Framework (n 10) 24-25.
[91] ibid.
[92] ibid 26.
[93] ibid 29.
[94] ibid.
[95] ibid 30.

sector, and that private businesses, especially SMEs, may not be capable of soliciting funds, recruiting human resources, and pooling skills to ensure interoperability.

Two recent reports have somewhat coincidentally espoused common standards as a way of achieving data interoperability. Commissioned by the European Commission, the Vestager report notes the limitations of Art 20 not a proper vehicle for delivering data portability and interoperability.[96] Similarly, the UK Government-commissioned Furman report recommends greater personal data mobility, and emphasises the relevance of open standards to this end.[97] Partly because of their focus on competition, both reports go beyond the remit of data protection and propose remedies to reinforce the right to data portability. The Vestager report points out that the GDPR has not be designed for continuous data access but simply as a means to get a copy of 'accumulated past data'. Without data interoperability, this right falls short of supporting multi-homing or innovative and complementary services building on top of the incumbent ones.[98] Two ways of remedy have been suggested to consolidate the right to data portability for its impacts on competition. On the one hand, data interoperability could be further facilitated by sector-specific legislation as in the Payment Service Directive. On the other, competition authorities may have a role in compelling the dominant firms to ensure data interoperability.[99] The Furman report offers a package of further actions. First, it proposes a digital markets unit that sets out a code of conduct for dominant firms. As part of this initiative, the firms are expected to agree on common standards in data portability and interoperability. Second, both data mobility and open standards are considered as useful tools to boost competition, and there is an obvious link between the two proposals. The attempt to achieve

[96] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the Digital Era' (European Commission-commissioned Report, 2019).
[97] Jason Furman and others, 'Unlocking digital competition: Report of the Digital Competition Expert Panel' (Digital Competition Expert Panel, March 2019) 5.
[98] Vestager Report (n 95) 8.
[99] ibid 9.

data portability through open standards is explicit as Open Banking is seen as 'an instructive example of policy intervention'. [100]

In sum, there is a drive towards interoperability by means of setting common standards at both EU and UK levels, fuelled by the development of competition policies. Standardisation process, if well-organised, is sensible in terms of allowing the stakeholders to participate in and agree on the underlying architectures that could benefit all. It appears as an obvious choice given the discrepancies of various kinds and the consequential difficulties in achieving semantic interoperability at the semantic level. However, given the discussions here have already gone beyond the context of Art 20 GDPR, a strong advocacy of common standards runs the risks of contravening the principle of proportionality and technological neutrality. As interoperability could be achieved pragmatically, data controllers may have legitimate grounds not to follow standardisation, a relatively demanding approach to interoperability with unforeseen implications for the market. More fundamentally, it begs the question as to whether interoperability is socially desirable or not.

However, As Palfrey and Gasser warn, wrong levels of interoperability can lead to uniformity/homogeneity and common standards have a levelling effect i.e. a powerful platform may set a standard that other stakeholders in the market are somehow compelled to align with and thereby unable to incorporate technological innovation. [101] Given that there are multiple ways to connect systems other than standardisation, and that the idea of interoperability is inherently concerned with a diversity of systems not necessarily the same, but able to work together, it cannot be too cautious to ensure that common standards for boosting competition do not lead to a reduction of diversity, which is eventually hazardous to that purpose pursued.

## Conclusion

This Chapter shows that technical hurdles can be as substantial as legal barriers in affecting the effectiveness of data portability. To ensure that data can be seamlessly transmitted between systems and well adapted to a new

[100] Furman Report (n 96) 5.
[101] Palfrey and Gasser (n 2) 106-7.

environment, the guidelines from competent authorities can play an important role in removing the hurdles identified in a technologically neutral and proportionate manner.

As shown previously, the EU Guidelines offer inconsistent and even conflicting guidance and the requirements of interoperability at each level remain ambiguous. This is primarily because interoperability, as a technical concept, has been used in the legal context without due consideration of its layered nature and the functionality difference between each layer. To bridge the discussions in the fields of technology and law, this Chapter uses this layered way of thinking to reconstruct the A29WP guidelines so as to bring in some technical clarity. Three major conclusions are made below. First, interoperability is not a legal mandate at the transport level, according to the A29WP Guidelines. Apart from interoperability-based solutions, the Guidelines should sufficiently acknowledge various other ways to deliver data portability and make room for data controllers to choose the optimal one. Second, interoperability at the syntactic level is explicitly prescribed by the GDPR provisions as well as the A29WP Guidelines. However, these requirements do not necessarily ensure that the syntaxes used by participating systems are compatible with each other. In this regard, the A29WP's path dependent approach should be treated with particular caution. As Palfrey and Gasser rightly warn, 'path dependency and legacy problems have complicated rather than enriched the process of setting an optimal level of portability or interoperability in history'.[102] Whereas the use of open formats is a standard in the public sector, it is not required by the GDPR at all. The advocacy of open format should not rule out the use of proprietary formats, which would clearly be in violation of the GDPR principles such as technology neutrality and proportionality. While experiences from public sector do provide useful lessons, sufficient room should be reserved for data controllers to decide, adapt and evolve. Last, it is suggested that the issue of interoperability at the metadata level be duly addressed, and that the provision of metadata be prescribed on

[102] Palfrey and Gasser (n 2) 157.

a proper legal basis. In the evolving legal landscape exist several grounds on which metadata should be provided, and the GDPR appears not a suitable one. As the Digital Content Directive is now put in place, the EDPB should alter the relevant portions of the A29WP Guidelines accordingly.

In a view to developing interoperability standards, there are three emergent frameworks respectively from the technology industry (currently involving only a few tech giants), government-endorsed research project (led by the Open Data Institute) and from the European Union (as part of the ISA2 Programme). All the solutions are characterised by a set of shared principles such as openness, reciprocity, user-centricity, among others. When it comes to implementation-level standards, however, reaching an industry-wide consensus is still a challenge. As a result, all the attempts conclude with the calls for multi-stakeholder dialogues.

| Framework | Open banking standards | Data Transfer Project | The New European Interoperability Framework |
|---|---|---|---|
| Nature | Government-endorsed | Industry response | Statutory |
| Established since | 2016- | 2018- | 2017- |
| Scope | All sectors | Private sector only | Public sector only |
| Background | Fingleton Report (2014) | Possibly resulted from the GDPR compliance | ISA2 programme (2016-2020) |
| Objectives | Consumer control over data; data access and reuse by FinTechs and other businesses; competition in banking | Service-to-service interoperability; industry-wide data portability | Interoperability between European public administrations |

| Focus | Open API | Adapter-based transfer | Semantic interoperability |
|---|---|---|---|

Table 5.3 Different Modes of Interoperability

Given the walled gardens are still a pertinent description for the current data ecosystem, the Data Transfer Project favours a pragmatic approach to interoperability. The White Paper prioritises the use of adapters by the participants without major changes to their core architectures.[103] In contrast, open banking appears to develop a data trust managed by the ODI, which would benefit all the organisations involved. The European interoperability framework has been developed for years, and a recent report made a response to the A29WP's reference to the relevance of works already established under the ISA2 programme.

Both schemes have shown the difficulties in reaching community-based consensus. First, the DTP could be seen as resulting from the pressure under the GDPR for responding to data portability requests. It brings forth a set of standards and invite other businesses to join. However, it appears that not all businesses are as interested as these tech giants at the forefront of GDPR compliance. Many challenges to reach a wider consensus have been flagged in the White paper, but it is the other business' call to commit and compete. The DTP original members are quite open to invite new participants but, due to the demands for funding, expertise and resources, the project has not yet achieved the level of impacts in the industry as expected.

Second, the EIF advocates the relevance and feasibility of its Core Vocabularies developed, and Core Persons in general, a set of semantic vocabularies for describing a person's basic identities. However, public administrations are generally not obliged to respond to data portability as they have exclusive legal bases for data processing, that is, public interest and function of public authority. As a result, the EIF-commissioned report is written only with the public sector in mind, and the limited circumstances where

[103] Data Transfer Project, 'Overview and Fundamentals' (DTP Whitepaper, 20 July 2018) 5.

authorities in rely on consent or contract for data processing in particular. Apart from pointing to the relevance of Core Persons, the rapporteurs advice active participation for legitimate requests, and call for multi-stakeholder discussions. It should be noted that these resources developed for public service delivery are unlikely to be accepted and adopted in the public sector, and that the EU does not have a legitimate ground for pushing these standards beyond the public sector.

Third, it is unreasonable to expect each of them to build their only facilities for data interoperability. The DTP White Paper has pointed out this dilemma between different deployment models and each has its advantages and drawbacks. It appears that the data trust model currently promoted by the ODI stands as a possible way forward. With an independent third-party serving as the Host Platform, all businesses, SMEs included, could simply write and maintain an adapter to connect with systems operated by others to ensure data portability. However, a number of other issues follow instantly, relating to trustworthiness, sustainability, scalability and source of funding. It appears that the challenge to achieve data interoperability does not primarily come from the data controllers and the final solution relies on coordinated efforts of all stakeholders. Specific problems have been left to data controllers, which cannot be addressed without community consensus. For instance, the DTP suggests a 'pull model'[104], that is, that a data subject should initiate the data transfer from the end of new data controller (data recipients). However, many controllers, especially SMEs, falls short of resources or skills to accept and adapt user data, or have not yet prepared for the incoming data.[105]

As interoperability could be achieved pragmatically, data controllers may have legitimate grounds not to follow standardisation, a relatively demanding approach to interoperability with unforeseen implications for the market. More

[104] ibid 24.
[105] Regarding the preparedness of businesses in Europe, see Michele Moore, 'Championing Data Protection and Privacy: A Source of Competitive Advantage in the Digital Century' (Capgemini, 26 September 2019) < https://www.capgemini.com/gb-en/news/data-protection-and-privacy-report/>accessed 7 October 2019.

fundamentally, it begs the question as to whether interoperability is socially desirable or not. However, As Palfrey and Gasser warn, wrong levels of interoperability can lead to uniformity/homogeneity and common standards have a levelling effect i.e. a powerful platform may set a standard that other stakeholders in the market are somehow compelled to align with and thereby unable to incorporate technological innovation.[106] Given that there are multiple ways to connect systems other than standardisation, and that the idea of interoperability is inherently concerned with a diversity of systems not necessarily the same, but able to work together, it cannot be too cautious to ensure that common standards for boosting competition do not lead to a reduction of diversity, which is eventually hazardous to that purpose pursued.

From a privacy perspective, interoperability is not obviously desirable. Palfrey and Gasser has described interoperability wholly as a source of threats to security and privacy.[107] System connectivity means more points of data access and would render the system vulnerable to bad actors.[108] Best and Pane echoes the potential intrusion into privacy resulting from the connections between systems.[109] In addition, they point to the plus side of interoperability for privacy that centralisation may bring forth 'better safeguards, sound access control policies, improved encryption, stronger privacy policies, and power to identify and address issues'.[110] It should be borne in mind that these benefits may only be real *within* a network of connected systems only. Given the fragmentation of the entire data ecosystem, with each undertaking building a walled garden against access of others, the threats to privacy posed by connected systems appear more prominent than these conceptual benefits.
The vulnerability of privacy and security within networks results from 'the increased complexity of an interoperable framework'.[111] It is not interoperability

[106] Palfrey and Gasser (n 2) 106-7.
[107] Palfrey and Gasser (n 2) 75-88.
[108] ibid.
[109] Katharina Best and John Pane, 'Privacy and Interoperability Challenges Could Limit the Benefits of Education Technology' (Rand Perspectives, October 2018) <https://www.rand.org/pubs/perspectives/PE313.html>accessed 11 October 2019.
[110] ibid.
[111] Palfrey and Gasser (n 2) 76.

itself that gives rise to increased privacy risks but, rather, the specificities of its implementation. The problem of privacy and security signifies the importance of the degree of interoperability - it is not binary - the right question to ask is hence the degree of interoperability desired ('selective interoperability'). Eventually our focus should be on the level of interoperability desired to ensure the desired level of security.[112]

Privacy and security is just one part of the whole picture. Even privacy-enhancing forms of interoperability may be challenged on the grounds of other important values, such as competition. While interoperability may bring to one consumer benefits, the level of interoperability producing an anticompetitive effect may eventually have a negative impact on consumer welfare overall.
From the competition perspective, the desirability of interoperability is not straightforward as well. In general, higher level of interoperability may lead to more competition, as evidenced in the Microsoft case.[113] There could be good competition, however, when the systems involved are not interoperable at all.[114] Essentially, the question about the desirability of interoperability would always be shifted to the degree of interoperability desired in a specific context. In any event, perhaps what we don't desire is a reduced diversity of products and services in the market, a negative impact of interoperability achieved through common standards. Given that there are multiple ways to connect systems other than standardisation, and that the idea of interoperability is inherently concerned with a diversity of systems not necessarily the same, but able to work together, special caution should be given to the standard-based approach to interoperability. This is somehow absent in both recent reports on the role of data portability in facilitating competition and should be remedied in future research.[115]

---

[112] ibid 81.
[113] Commission Decision of 27 February 2008 (Case COMP/C-3/ 34.792 – Microsoft). See also Stefano Barazza, '(European) Commission v Microsoft: How to Set Reasonable Rates for Access to Interoperability Information and Evaluate their Innovative Character?' (2013) 4(1) Journal of European Competition Law & Practice 55-58.
[114] Palfrey and Gasser (n 2) 98.
[115] Furman Report (n 96). Vestager Report (n 95).

# Chapter 6 The Quest for Data Utopia: A Survey of User-Centric Technologies for Better Protection of Personal Data

## Introduction

In the digital age, businesses, policymakers and media have zealously framed data as the 'the new oil'[1] or the 'new currency'.[2] The true value of data is, however, not often straightforward to average individuals, now put in a more prominent position to access, control and reuse their data. After the GDPR and other EU instruments tear down the 'walled gardens' of data controllers, there exists an increasing number of tools for making data portability request.[3] Given that data access/export is no longer a problem, and data reuse technically feasible, individuals who seek their data are still facing challenges to make use of them meaningfully and effectively. In their eyes, data obtained through the GDPR are nothing but a mix of numbers, tables, and files, as several anecdotes reveal.[4] In many cases, the value of complex, technical datasets is

[1] 'The World's Most Valuable Resource is No Longer Oil, but Data' (The Economist, 6 May 2017) available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>accessed 14 May 2019. See also Antonio García Martínez, 'No, Data Is Not the New Oil' (WIRED, 25 February 2019) available at <https://www.wired.com/story/no-data-is-not-the-new-oil/>accessed 14 May 2019.

[2] William D. Eggers and others, 'Data as the New Currency' (Deloitte Insights, 24 July 2013) available at <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html>accessed 14 May 2019. See also 'Data is the New Currency' (KPMG, 20 November 2018) available at <https://home.kpmg/im/en/home/insights/2018/11/data-is-the-new-currency.html>accessed 14 May 2019. Natarajan Chandrasekaran, 'Is Data the New Currency?' (WEF Agenda, 14 August 2015) available at < https://www.weforum.org/agenda/2015/08/is-data-the-new-currency/>accessed 14 May 2019. Luke Stark and Anna Lauren Hoffmann, 'Data Is the New What? Popular Metaphors and Professional Ethics in Emerging Data Culture' (2019) Journal of Cultural Analytics, available at <https://culturalanalytics.org/2019/05/data-is-the-new-what-popular-metaphors-professional-ethics-in-emerging-data-culture-2/>accessed 14 May 2019.

[3] For instance, My Data Request is an online tool that processes Privacy Policies of over 100 data controllers and codifies the request process for data subjects to acquire their data. See My Data Request, available at <https://mydatarequest.com>accessed 14 May 2019. See also Janis Wong and Tristan Henderson, 'How Portable is Portable? Exercising the GDPR's Right to Data Portability' (UbiComp/ISWC'18 Adjunct, October 8–12, 2018, Singapore).

[4] Sara Ashley O'Brien, 'I Downloaded 14 Years of my Facebook Data and Here is What Happened' (CNN, 25 March 2018) available at <https://money.cnn.com/2018/03/24/technology/facebook-data/index.html>accessed 14 May 2019. See also Josh Constine, 'Friend Portability is the Must-have Facebook Regulation' (TechCrunch, 12 May 2019) available at <https://techcrunch.com/2019/05/12/friends-

extractable only with resources, knowledge and skills that most individuals do not have. Apparently, they need further assistance from third-party specialists, empowerment by user-centric technologies, as well as the guidelines from data protection authorities.

This chapter surveys user-centric technological systems emerged over two decades (1999-2019). As the GDPR right to data portability would interface well with these systems, it inquires to what extent the combined effort of law and technology would bring us better protection and management of personal data.

The chapter consists of four parts. Part 1 provides an overview of EU policies promoting a higher level of interaction between law and technology. The right to data portability itself might not be sufficient to help data subjects protect or reuse personal data. As suggested by those policies, the right should be used in tandem with technologies that genuinely put individuals in the centre of data management. Part 2 maps several concepts that have provisionally inspired the development of user-centric technologies. A trajectory of conceptual development is noted from user empowerment to human-based agents and then to user-centric technological systems. Part 3 surveys a selection of 12 user-centric technological systems, which potentially represent the future of data protection and management but struggle to compete against popular services and direct data inflows. Part 4 provides some reflections upon the evolution of technological systems over the two decades (1999-2019) and their potential interaction with legal rights recently created.

---

wherever/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=2XPb9v3gGAl50uJ77kTKTw>accessed 14 May 2019. Jon Porter, 'GDPR Makes it Easier to Get Your Data, but that Does Not Mean You Will Understand it: 138 GB of data and No Real Answers' (The Verge, 27 January 2019) available at <https://www.theverge.com/2019/1/27/18195630/gdpr-right-of-access-data-download-facebook-google-amazon-apple>accessed 14 May 2019. Arjun Kharpal, 'Facebook Rolled out Privacy Changes — but it's Being Forced to Do it Anyway by Regulators' (CNBC, 29 March 2019) available at<https://www.cnbc.com/2018/03/29/facebook-has-rolled-out-privacy-changes--but-its-doing-it-for-gdpr.html>accessed 14 May 2019.

# I. The Role of Technologies in Data Protection: The EU Initiatives

The combined use of law and technology for data protection and management has been cogently expressed in numerous EU documents. The European Commission, for instance, encourages the use of 'personal data spaces as user-centric, safe, and secure places to store and possibly trade personal data'.[5] To this end, the Commission supports research and innovation on digital tools that 'assist users in selecting the data sharing policies that best match their needs'.[6] Similarly, the European Data Protection Supervisor contends that 'innovative digital tools and business models based on consumer empowerment should be encouraged'.[7] In his Opinion on Big Data, the EDPS suggests that 'personal data spaces' be built upon data portability for continuously storing real-time big data.[8] In another opinion, the EDPS further facilitates the creation of 'a new reality where individuals manage and control their online identity'.[9] In this new landscape, business models that collect and process personal data 'in a manner more respectful of European data protection law' are particularly supported.[10]

Notably, the right to data portability in the GDPR is mentioned as a contributor to 'the more efficient market for personal data'.[11] In connection to this, the EDPS argues that coherent enforcement of fundamental rights would create market conditions in which privacy-friendly services can thrive.[12] The Article 29 Working Party (A29WP), when interpreting the right to data portability, also

---

[5] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-driven Economy' COM(2014) 442 final, 2.7.2014, p.11.
[6] ibid.
[7] European Data Protection Supervisor, 'Opinion on Meeting the Challenges of Big Data: A Call for Transparency, User control, Data Protection by Design and Accountability (Opinion 7/2015, 19 November 2015) 13-4.
[8] ibid.
[9] European Data Protection Supervisor, 'Opinion on Personal Information Management Systems' (EDPS Opinion 9/2016, 20 October 2016) 3.
[10] ibid.
[11] ibid.
[12] European Data Protection Supervisor, 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (EDPS Opinion 8/2016, 23 September 2016) 12-4.

alludes to the use of personal data stores, personal information management systems or other kinds of trusted third parties.[13]

## II. Underlying Concepts

This section provides an account of concepts that have enriched or inspired the emergence of user-centric technological systems. These concepts build upon, or overlap with, each other. A trajectory of conceptual development can be seen from technological empowerment (Privacy by Negotiation) to human-based assistants (infomediaries) and then to automated tools (Personal Data Stores and Vendor Relationship Management).

### 1. Technological Empowerment and Privacy by Negotiation

Around the 1990s, the idea of Privacy by Negotiation (or 'Negotiated Privacy') emerged as a response to standardised offers that discouraged consumers. For instance, Tubaro suggests a departure from Warren and Brandeis' right to be left alone, what he conceptualises as 'privacy as penetration'.[14] In its stead, Tubaro proposes a model of privacy as negotiation, understood as 'a gradual process of individual adaptation to signals from the social environment'.[15] As Dix contends, the underlying rationale behind negotiated privacy is that every user can negotiate on the Privacy Policies and Terms of Uses that apply to him.[16] Individuals themselves may have to negotiate on the use of their 'shared' data (*e.g.* a group photo) as well. Should every user get an individualised contract, the use of personal data is tailored to specific individual preference. As Preibusch argues, the Privacy-by-Negotiation technique also evades the

[13] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 16.
[14] Paola Tubaro, 'Why Online Privacy is Not Dead: Negotiation and Conflict in Social Media' (Discover Society, 15 February 2014) available at<https://discoversociety.org/2014/02/15/why-online-privacy-is-not-dead-negotiation-and-conflict-in-social-media/>accessed 8 May 2019.
[15] ibid.
[16] Alexander Dix, 'Infomediaries and Negotiated Privacy Techniques' (The Tenth Conference on Computers, Freedom and Privacy, New York, 2000) 167.

consequences that consumers frustrated by 'take-it-or-leave' offer choose to avoid online interaction and become detached from the cyberspace.[17]

That said, the disparities between individuals in valuing their privacy should never be underestimated. As Empirical research shows, differences exist between individuals in the desired degree of information disclosure and their expectation of privacy.[18] Not all individual users are willing to negotiate, and some even do not have the knowledge, time, or capacity to bargain with vendors. To address these issues, Such and Rovatsos argue for heuristics as a way of reducing the negotiation complexities. They demonstrate with an experiment that heuristics, which provide rapid negotiation process, can be effectively used on social media infrastructure.[19] Further, Tubaro and others contend that a dynamic process of negotiation, including signalling, listening, adapting, among others, can be construed through agent-based computer simulation.[20] The Negotiated privacy technique has recently been a topical theme in the field of Internet of Things (IoT) as well. Alanezi and Mishra, for instance, develop a mechanism that allows IoT users to express and enforce their privacy preferences while interacting with IoT deployments.[21]

### 2. Assistance from Human Specialists: the Rise of the Infomediary

Towards the end of the 20th century, another concept of information intermediary, or infomediary, emerged as a supplement to negotiated privacy. Basically, infomediaries interface between the consumer and the business,

---

[17] Sören Preibusch, 'Key Facts on Privacy Negotiations' (Sören Preibusch's Personal Blog, 2009) available at <http://preibusch.de/#pn>accessed 19 February 2019.
[18] Federico Morando and Emilio Raiteri, 'Privacy Evaluation: What Empirical Research on Users' Valuation of Personal Data Tells Us' (2014) 3(2) Internet Policy Review 1. Kirsten Martin, 'Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online' (2015) 34(2) Journal of Public Policy and Marketing 210. Meredydd Williams and Jason Nurse, 'Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective' (Lecture Notes in Computer Science, Vol. 9750, 2016) 186-197.
[19] Jose Such and Michael Rovatsos, 'Privacy Policy Negotiation in Social Media' (2016) 11(1) ACM Transactions on Autonomous and Adaptive Systems Art 4, 1.
[20] Paola Tubaro and others, *Against the Hypothesis of the End of Privacy: An Agent-based Modelling Approach to Social Media* (Springer International 2014)
[21] Khaled Alanezi and Shivakant Mishra, 'A Privacy Negotiation Mechanism for IoT' (IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, Athens, Greece, 29 October 2018).

specialising in managing data and negotiating with vendors on behalf of consumers.[22] In the book *Net Worth*, Hagel and Singer first express the idea and call the infomediaries 'brokers for consumer information'.[23] They believe that infomediaries would exchange personal data on behalf of consumers while at the same time preserve consumer privacy.[24]

### 3. Trust in Machines: Personal Information Management System (PIMS)

In contrast to human-based agents, the idea of automated intermediation emerged as early as the infomediary model was conceived. For instance, Hagel and Rayport, who coined the concept of infomediary, pin hope on technologies. They argue that infomediaries would 'play a very traditional role...in negotiating the best deal for consumers'.[25] Beyond this, technologies have the potential to relocate our personal data and then reorganise them in systems centred on individuals.[26] Goldman envisions that software agents would make marketing messages highly relevant; ultimately, these machine-based agents would help achieve the optimal level of marketing (known as the Coarsen filter).[27] Narayanan and others note that the first generation of infomediaries had rapidly floundered in the early 2000s, followed by a wave of new projects featuring the use of user-centric technologies.[28] These technologies have the potential to eliminate the need to outsource data management to trusted human agents.

Kang and others propose a 'Personal Data Guardian' (PDG) model as an alternative to infomediary. PDG differentiates itself from earlier attempts by

[22] John Hagel III and Mark Singer, *Net Worth: Shaping Markets When Customers Make the Rules* (Harvard Business School Press 1999) 21.
[23] ibid 19.
[24] ibid.
[25] John Hagel III and Jeffrey Rayport, 'The Coming Battle for Customer Information' (Harvard Business Review, January-February 1997), available at <https://hbr.org/1997/01/the-coming-battle-for-customer-information>accessed 17 February 2019.
[26] ibid.
[27] Eric Goldman, 'A Coasean Analysis of Marketing' (2006) Wisconsin Law Review 1151, 1202.
[28] Arvind Narayanan and others, 'A Critical Look at Decentralized Personal Data Architectures' (2012) arXiv:1202.4503v1 [cs.CY].

storing data in a place called ‘Privacy Data Vault’, which is entirely under a user’s control.[29] A Kang and others put it, whereas infomediaries functions as ‘commercial middleman’, PDG are in essence ‘trustees or faithful agents’.[30] This is epitomised by a set of rules embedded in this model to restrict data access and reuse, notably including a fiduciary relationship between the user and the PDG. As a fiduciary, a PDG must demonstrate a minimum competence, reveal no confidences and owe a duty of loyalty to the user.[31]

Personal Information Management System (PIMS) is a concept more commonly used in recent times. It can be traced back to the 1980s when the rise of personal computer brought hope to humans that their capacity would be significantly enhanced.[32] Since then, PIMS has been extensively explored as an independent field of inquiry. This concept primarily covers two categories of technologies: some are inherently centralised, with an operator in the centre of system; others notably feature a decentralised architecture, creating space for human autonomy. These two categories of technological systems will be explained in turn.

The World Economic Forum (WEF) explores the centralised model of PIMS through its Rethinking Personal Data Project. This project aims to examine aspects of ‘a principled, collaborative and balanced personal data ecosystem’.[33] In a report on PIMS and user empowerment, the WEF coined the term ‘user-centricity’ as a cure for the ‘fragmented and inefficient personal data ecosystem’.[34] To this end, consumer trust and contextual integrity are considered the key methods of governance.[35]

[29] Jerry Kang and others, ‘Self-Surveillance Privacy’ (2011) 97 Iowa Law Review 809, 837.
[30] ibid 829-30.
[31] ibid 832.
[32] Mark Lansdale, ‘The Psychology of Personal Information Management’ (1988) 19(1) Applied Ergonomics 55.
[33] World Economic Forum, ‘Personal Data: The Emergence of a New Asset Class’ (2011).
[34] ibid.
[35] World Economic Forum, ‘Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems’ (May 2014).

Another concept of 'Personal Data Store', also known as 'vault', 'place', 'locker', 'cloud', etc., is used often in practice. These concepts refer to a wide array of technological systems existing in the market that 'empower individuals to control the collection and sharing of personal data'.[36] There exists one particular strand of PDS characterised with decentralised architecture, meaning that data is stored and processed 'locally' (*i.e.* on the user's computer or mobile phone), as opposed to being hoarded by a centric controller.

### 4. An Integrated Solution: Vendor Relationship Management

Building on PIMS, Vendor Relationship Management (VRM) represents an integrated solution to help consumers 'obtain independence from the vendors' on the one hand, and provide 'consumers with better means to engage with vendors' on the other.[37] As Mitchell and others put it, VRM '[eliminates] the infomediary as a separate entity, and instead [replaces] it with a software agent'.[38] The WEF also sees VRM as an extension to PIMS or PDS because it 'realises direct value - money or in kind - from the personal data stored'.[39] First appeared in the magazine ComputerWorld 2000[40], the concept of VRM was systematically examined by Doc Searls in his ProjectVRM.[41] This project aims to transform the Customer Relationship Management (*i.e.* the annoying and inefficient system that many companies use to manage their relationship with customers), along with many problematic ideas associated with it, such as 'target', 'capture', and 'lock-in'.[42] Searls believes that most marketing problems should be addressed from the consumer side (demand) rather than the vendor side (supply). In his book *Intention Economy*, he anticipates that technologies would lead us to the shift from buyers finding sellers (e-

[36] EDPS (n 7) 13-4. See also Ira S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74, 82.
[37] Doc Searls, 'Our Time Has Come' (ProjectVRM, 16 May 2018) available at <http://blogs.harvard.edu/vrm/2018/05/16/time>accessed 19 February 2019.
[38] Alan Mitchell, Iain Henderson and Doc Searls, 'Reinventing Direct Marketing — With VRM Inside' (2008) 10(1) Journal of Direct Data and Digital Marketing Practice 3–15.
[39] World Economic Forum, 'Personal Data: The Emergence of a New Asset Class' (2011) 30.
[40] Michael Cohn, 'Open Wide for More Tech-World Alphabet Soup' (ComputerWorld, 1 May 2000) 36.
[41] Project VRM (Berkman Klein Center, 2 February 2019) available at <https://cyber.harvard.edu/projectvrm/Main_Page>accessed 15 May 2019.
[42] ibid.

commerce) to sellers finding buyers (i-commerce).[43] This fundamental shift has also been concisely expressed, for instance, in a CtrlShift report on the new landscape of personal data:

*For the last 50 years, technological advances have provided organisations with a growing array of tools and services to gather, store, analyse and use information about their customers. These developments have created an organisation-centric data environment, where organisations are the managers and users of customer data and customers are relegated to the role of passive 'subject' and target of organisations' data-driven activities… Two trends – individuals managing and using information as a tool in their own hands, and individuals as the point of integration of information about their own lives – are transforming the personal data landscape. [44]*

Rubinstein is an outspoken advocate of VRM-equivalent models. He argues that the 'informed choice model is broken beyond any regulatory repair'.[45] The only way forward is to combine legal reform with 'new business models premised on consumer empowerment'.[46] In his view, new models even have the potential to render data protection principles 'efficacious' as they give the individuals the capacity to benefit from Big Data and learn how to control.[47]

## III. The Rise and Fall (and Rise?) of User-centric Technologies

Inspired by the concepts examined above, an increasing number of products have been established since the end of the 20th century. This section provides a survey of projects within a timespan of two decades (1999-2019). A total of 12 projects are examined. To note, this is not an exhaustive list, and many other systems are being built all over the world.[48] This selection aims to demonstrate the variations of motives, functionalities, and the need for data

[43] Doc Searls, *The Intention Economy: When Customers Take Charge* (Harvard Business Review Press 2012) 41.
[44] CtrlShift, 'The New Personal Data Landscape' (Ctrl-Shift, November 2011) 4.
[45] Rubinstein (n 36) 79.
[46] ibid 74.
[47] ibid.
[48] For instance, a much more comprehensive list of projects, products and services across the world may be found at VRM Development Work, available at <https://cyber.harvard.edu/projectvrm/VRM_Development_Work>accessed 1 June 2019.

portability. To this end, this section particularly entails projects stimulated by the General Data Protection Regulation (GDPR) and those featuring the use of new technologies such as Application Programming Interface (API), blockchain and artificial intelligence (AI).

### 1. All Advantage (1999-2001/2006)

Launched in 1999, AllAdvantage claimed to be the first infomediary across the globe. This project was well-known for its business model, *i.e.* 'pay to surf the web'.[49] Basically, advertisements were displayed by a viewbar on a user's screen, based on the contents being viewed by that user. Within two months after inception, AllAdvantage paid out 10 million USD of its advertising revenue to its members.[50] In 2001, the company was reportedly affected by the financial concession and, by the time of the closure of consumer-facing operations, it had paid out more than 160 million to its users.[51] Reportedly, AllAdvantage 2.0 shortly re-appeared in 2006 under the name of AGLOCO.[52]

- *Data Collection*: The AllAdvantage's viewbar software passively monitored online activities and users did not have to volunteer any personal information
- *Individual Control*: Users were not allowed to decide on the price of information or the types of advertisements displayed.
- *Data Use/Added Value*: AllAdvantage adopted an unprecedented advertisement-based business model, paying a portion of revenue to its users (up to 53 US cents per hour).[53]

[49] 'AllAdvantage Pays out over $10,000,000 in 2 Months' (Geek, 16 December 1999) available at <https://www.geek.com/news/alladvantage-pays-out-over-10000000-in-2-months-566599/>accessed 7 May 2019.
[50] ibid.
[51] 'AllAdvantage Pays out over $10,000,000 in 2 Months' (Geek, 16 December 1999) available at <https://www.geek.com/news/alladvantage-pays-out-over-10000000-in-2-months-566599/>accessed 7 May 2019. Lisa Guernsey, 'Can It Pay to Surf the Web?' (New York Times, 1 July 1999) available at<https://www.nytimes.com/1999/07/01/technology/can-it-pay-to-surf-the-web.html>accessed 7 May 2019.
[52] John Chow, 'AllAdvantage 2.0 – Get Paid To Surf The Net' (John Chow, 22 November 2006) available at <https://www.johnchow.com/alladvantage-20-get-pay-to-surf-the-net/>accessed 7 May 2019.
[53] David Cotriss, 'Where Are They Now: AllAdvantage.com' (The Standard, 30 June 2008) available at <http:/thestandard.com/news/2008/06/30/where-are-they-now-alladvantage-com>accessed 17 February 2019.

### 2. Lumeria (1999-)

Lumeria was one of the earliest infomediaries helping individuals manage their personal data. Fred Davis, the CEO of Lumeria, sought to build 'revolutionary technologies' in addressing the problem of the internet becoming 'the worse of all places for unwholesome invasions of people'.[54] The so-called SuperProfile system, once fully built, would allegedly 'make the Fair Information Principles redundant'.[55]

- *Data storage*: In the centre of Lumeria lies the SuperProfile system, a profiling system enabling the users to 'own' their data and keep them private - even Lumeria does not have access 'without consent'.[56] Unfortunately, the Lumeria white paper fails to express how this is to be technically implemented.
- *Data access/use*: the SuperProfile system was meant to allow users to appoint agents who use the data to find the best deal.[57] The appointed agents can be Lumeria itself or any other third parties. Lumeria was committed to engaging into the Identity Commerce (I-commerce), a market where traders compete for a consumer's need with discounts, extra perks, better services, good deals and even money.[58] Therefore, its business model depends upon users actively trading their identities for 'benefits, convenience and profits'.[59]

### 3. The Platform for Privacy Preferences (2002-)

The Platform for Privacy Preferences (P3P) is a protocol developed by the World Wide Web Consortium (W3C). It is an automated way for users to understand privacy policies and gain control over the use of their personal data.[60] P3P enables the websites to express their privacy policies in a machine-readable format so that these policies can be automatically retrieved, processed and interpreted. As a result, users don't need to read these policies and would be immediately alerted when a website's conflicts with his or her

---

[54] James Glave, 'The Dawn of the Infomediary' (WIRED, 24 February 1999) available at <https://www.wired.com/1999/02/the-dawn-of-the-infomediary/>accessed 11 May 2019.
[55] Fen Labalme and Jad Duwaik, 'An Infomediary Approach to the Privacy Problem' (Broadcatch, February 1999) 10.
[56] ibid.
[57] ibid.
[58] ibid.
[59] Lumeria, 'What is A SuperProfile', available at <https://superprofile.net/sprofile.html>accessed 13 May 2019.
[60] 'P3P 1.0: A New Standard in Online Privacy' (W3C, 12 May 2006) available at <https://www.w3.org/P3P/brochure.html>accessed 8 May 2019.

privacy preferences. P3P is operated on a voluntary basis and, unfortunately, there were very few websites in support of it. The CyLab 2006 report shows that, among the top 5000 websites, only 15% of them were P3P-enabled.[61] Mozilla briefly supported P3P features but removed related source codes in 2007.[62] Microsoft's Internet Explorer and Edge were the major browsers that supported P3P. After Microsoft ended support from Windows 10 onwards, however, P3P had become virtually obsolete.[63]

- *Data collection*: P3P requires that users create their own profiles to describe their privacy preferences. The user profile is stored on the browser(s) and can be automatically read by the website visited.

### 4. Mydex (2007)

Mydex builds its PDS for individuals to 'exchange personal data with confidence'.[64] In this store, users can manage their data 'in a highly secure and structured way'.[65] Additionally, they can 'acquire and reuse proofs of claims or of relationships and qualifications (such as bank account, verified address, driving licence or support)'.[66] Mydex has been closely associated with the UK's midata initiative. For instance, its ID Assurance Framework provides support for midata and fits in the Digital-by-Default Agenda for Universal Credit.[67] As the UK Government ceased to support Mydex as one of the

[61] Lorrie Cranor and others, '2006 Privacy Policy Trends Report' (CyLab Privacy Interest Group, 31 January 2007) 6.
[62] 'Remove P3P from the Default Build' (Bugzilla, 28 November 2007) available at <https://bugzilla.mozilla.org/show_bug.cgi?id=225287>accessed 7 May 2019.
[63] 'P3P is No Longer Supported' (Microsoft, 15 December 2016) available at <https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/mt146424(v=vs.85)>accessed 7 May 2019.
[64] Crunchbase, Overview of MyDex, available at <https://www.crunchbase.com/organization/mydex#section-overview>accessed 9 May 2019.
[65] Understanding Personal Data Stores (PDS) (MyDex, 1 October 2015) available at <https://web.archive.org/web/20151001065833/https://mydex.org/understand-pds/>accesed 7 May 2019.
[66] ibid.
[67] Mydex, 'Why Midata Matters' (Mydex Blog, 1 October 2015) available at <https://web.archive.org/web/20151001064341/https://mydex.org/why-midata-matters/>accessed 9 May 2019. See also The UK's Department for Work & Pensions, 'Digital Strategy' (Policy Paper, December 2012) 29-30. Tim Hill and David Alexander, 'Mydex Data Services CIC: The Third Sector and the Future of Stakeholder Engagement in Challenging Times' (Mydex Whitepaper, November 2012) 4, 41.

certified identity providers under GOV.UK Verify in 2015[68], the company now contributes through the Open Identity Exchange Forum.[69]

- *Data access*: Mydex's PDS is API-based, allowing the users to pull data in their stores and the external applications to establish connections.[70]

## 5. Higgins (2008-)

Higgins is a user-centric identity management system built to 'integrate digital identities, user profiles, and social relationship information across multiple sites, applications and services'.[71] It was funded by Eclipse Foundation and was part of the Social Physics project at Harvard Berkman Klein Centre.[72]

- *Data Storage*: Higgins 2.0 features the use of PDS, a cloud-based service enabling bidirectional data flows between it and external businesses or other PDSes.[73]
- *Data Use*: Higgins develops an interoperable infrastructure for 'Information-cards' (I-cards)[74], a graphical way to refer to a collection of identity information that a user intends to share with websites and applications. From the user's perspective, each I-card has a card-shaped picture and a card name. When a website wants to access user information, the visual cards appear to help the user manage his or her identities.[75]
- *Data Portability*: Higgins allows users to export data in a machine-readable format (*i.e.* Resource Description Framework).

---

[68] Janet Hughes, 'GOV.UK Verify and Mydex CIC' (GOV.UK Verify Blog, 25 March 2015) available at <https://identityassurance.blog.gov.uk/2015/03/25/gov-uk-verify-and-mydex/>accessed 9 May 2019.
[69] ibid.
[70] Tim Hill, Mydex Data Services CIC: The Third Sector and the Future of Stakeholder Engagement in Challenging Times (Mydex White Paper, November 2012) 47.
[71] 'Eclipse Releases Its First User-Centric Identity Framework' (Eclipse Foundation, 21 February 2008) available at <https://www.eclipse.org/org/press-release/20080221_higgins.php>accessed 7 May 2019.
[72] 'Past Project: SocialPhysics.org' (Berkman Klein Centre, 28 June 2018) available at <https://cyber.harvard.edu/research/socialphysics>accessed 11 May 2019.
[73] Higgins 2.0, available at <https://wiki.eclipse.org/Higgins_2.0>accessed 11 May 2019.
[74] Eclipse Foundation, 'Eclipse Higgins', available at <https://projects.eclipse.org/projects/technology.higgins>accessed 11 May 2019.
[75] Apart from Higgins, famous identity selectors also include Windows CardSpace and Digi.me. The Windows CardSpace (code-named InfoCard) was terminated in 2011 and Microsoft is working on a replacement called U-Prove. See Project UProve (Microsoft, 25 February 2012) available at <https://www.microsoft.com/en-us/research/project/u-prove/>accessed 12 May 2019.

### 6. ownCloud (2010-)

ownCloud claimed to be one of the largest open-source projects on data sync and sharing. It does not provide data storage service, so users have to operate ownCloud on their private server or cloud.[76] One of the ownCloud's major drawbacks is, as Urquhart and others argue, limited types of data supported, such as photos, status message, and hosting files. This poses challenges to data portability since 'applications are evolving to require diverse kinds of data' in the age of IoT.[77] ownCloud claims to be GDPR-compliant as all data is 'fully logged and exportable'.[78]

- *Data Storage*: ownCloud is a self-hosted, software-only product, meaning that the service does not offer (off-premises) data storage capacity. Users have to leverage their own storage such as FTP, Dropbox and Swift.[79]
- *Data access*: ownCloud is API-based, enabling data access through a user interface.[80] It also fully supports the Web Distributed Authoring and Versioning protocol (WebDAV), an extension to the Hypertext Transfer Protocol (HTTP).[81]

### 7. Personal/Digi.me (2009-/2017-)

Personal was a data management company founded in 2009. Shane Green, the CEO of Personal, describes it as the first 'Privacy by Design' company. Personal is also one of the earliest companies in the startup circle of the 'Personal Data Ecosystem Consortium'.[82] Inspired by Doc Searl's ProjectVRM, Personal was committed to building the world's first reverse license mechanism. Literally, it is assumed that data ownership resides with users and

---

[76] ownCloud features, available at <https://owncloud.org/features/>accessed 11 May 2019.
[77] Lachlan Urquhart, Neelima Sailaja, Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22(2) Personal and Ubiquitous Computing 317, 324.
[78] ownCloud, 'Information on the EU-General Data Protection Regulation (EU-GDPR)' (EU-DSGVO Whitepaper, 2 May 2018) available at <https://owncloud.com/gdpr>accessed 9 May 2019.
[79] ownCloud, 'ownCloud Features' available at <https://owncloud.org/features>accessed 12 May 2019.
[80] Urquhart and others (n 77) 324.
[81] ownCloud, 'Accessing ownCloud Files Using WebDAV' (ownCloud 8.2 User Manual), available at <https://doc.owncloud.org/server/8.2/user_manual/files/access_webdav.html>accessed 12 May 2019.
[82] Personal Data Ecosystem Consortium, 'Members of the PDEC Startup Circle', available at <http://pde.cc/startup-circle/#2011>accessed 11 May 2019.

that they have the right to licence access to third parties further. In 2017, Personal merged with Digi.me, a UK-based start-up.[83] The combined company (also called Digi.me) offers the so-called distributed user-centric architecture that has the potential to 'shift power to individuals'.[84]

- *Data storage*: Personal launched Data Vault (beta), a data storage service, in November 2011.[85] Digi.me does not store user data and relies on the user's personal cloud for storage.[86]
- *Data access and use*: Personal released its first API as early as October 2012.[87] The combined company Digi.me also enables automatic access and synchronisation through APIs.[88]

### 8. Locker Project (2012-)

Locker project aims to capture and archive 'data exhausts' online, that is, the crumbs of data users leave behind as they move around the web.[89] Singly, the sponsor of the Locker project, partnered with a peer-to-peer networking protocol called TeleHash in 2011. This partnership now provides an integrated solution to data management, control and reuse. Whereas the 'lockers' are built to store and manage data, TeleHash connects all the lockers and enable automatic data exchange between them.[90]

---

[83] Digime, 'What is Digi.me', available at <https://digi.me/what-is-digime/>accessed 9 May 2019.
[84] ibid.
[85] Ben Parr, 'Never Fill Out a Form Again? Personal Seeks to Be the Data Vault for Your Private Information' (Mashable UK, 18 November 2011) available at <https://mashable.com/2011/11/17/personal/?europe=true>accessed 9 May 2019
[86] Digi.me, 'How Do We Protect Your Data and Privacy?', available at<https://digi.me/privacy>accessed 11 May 2019.
[87] 'Personal Launches 'Personal Platform' at Business of APIs Conference' (Team Data, 2 October 2012) available at <https://teamdata.com/s/pages/news/personal-launches-personal-platform/>accesed 9 May 2019. See also Kin Lane, 'API Evangelist History of APIs' (API.Lessons, 10 April 2019) available at <https://history.apievangelist.com/>accessed 9 May 2019.
[88] Steve O'Hear, 'Digi.me and Personal Merge to Put You in Control of the Nascent "Personal Data Ecosystem"' (TechCrunch, 17 August 2017) available at <https://techcrunch.com/2017/08/17/digi-me-and-personal-merge/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=vasf1c48PqL5o27_wN2YGg>accessed 11 May 2019.
[89] Ryan Kim, 'The Locker Project: Why Leave Data Tracking to Others? Do It Yourself' (Gigaom, 4 February 2011) available at <https://gigaom.com/2011/02/04/the-locker-project-why-leave-data-tracking-to-others-do-it-yourself/>accessed 9 May 2019.
[90] Tish Shute, 'The Locker Project: Data for the People' (O'Relly Radar, 11 February 2011) available at <http://radar.oreilly.com/2011/02/singly-locker-project-telehash.html>accessed 9 May 2019.

- *Data Storage*: The Locker Project is PC-based (or client-based), meaning that attribute sets are placed on the user's computer.
- *Data Access*: The Locker Project uses API to pull in user data and enable external applications to connect with lockers.[91] The adoption of TeleHash protocol further connects lockers and enables peer-to-peer sharing.

### 9. HAT (2013-)

The Hub of All Things (HAT) is a multidisciplinary project to create a decentralised personal database for users to take back control of their data. Supported by the Engineering and Physical Sciences Research Council (EPSRC), HAT involves researchers from six British Universities. It is advertised that the HAT ecosystem is 'the first to fully resolve the technical, legal and commercial barriers in the ownership and transfer of personal data between individuals and organisations'. [92] Arguably, the HAT confers 'intellectual property rights of personal data to individuals through their ownership of a dedicated database'. [93] The third-party apps (called 'microservices') pay the royalties to users (called 'HAT owners') when using the data or insights generated.[94] Further, the HAT claims that this product is merely an infrastructure for apps and websites; as a result, HAT owners are supposed to be the data controller or processor in accordance with the GDPR.[95] This links back to the scenario explained earlier that an individual is likely to become a data controller by means of user-centric technologies.

- *Data storage*: HAT is a software-only product that does not provide storage capacity. The microserver is built on the cloud, and the microservices do not store the data.[96]
- *Data Access*: The HAT is integrated with third-party software called 'data plugs' for collecting data on the internet and pulling into the HAT

[91] Ryan Kim, 'The Locker Project: Why Leave Data Tracking to Others? Do It Yourself' (Gigaom, 4 February 2011) available at <https://gigaom.com/2011/02/04/the-locker-project-why-leave-data-tracking-to-others-do-it-yourself/>accessed 9 May 2019.
[92] HAT, 'The Hub of All Things: Own Your Own Personal Data', available at <https://www.hubofallthings.com/main/what-is-the-hat>accessed 9 May 2019.
[93] ibid.
[94] HAT, 'Introducing the Hub-of-All-Things (HAT) and the HAT Ecosystem', available at <https://static1.squarespace.com/static/5b5988f9b105985261c0a722/t/5c179df3f950b7d4a378c11b/1545051654456/hatpresentation1.7PDF.pdf>accessed 12 May 2019.
[95] ibid.
[96] HAT (n 92).

ecosystem. With microservices interoperate within the system through APIs, the HAT aims to achieving data interoperability 'across all sectors but fully in control of the individual'.[97]

- *Artificial Intelligence*: Notably, HAT introduces the Smart Engine (HSE) that 'take on new AI tools to analyse HAT data and create insights'.[98] Users can share these insights, as opposed to data, within other apps (called 'data debits').[99]AI-powered tools are pre-trained so that, unlike traditional AI model, data is not taken out of the HAT ecosystem.[100]

## 10. Solid/Inrupt (2015-/2018-)

Solid is an open-source project created by Sir Tim Berners-Lee, who intends to 're-orient the web to its original version'.[101] He notes that the web was meant to be a decentralised platform for everyone, but has been increasingly centralised against his original intention.[102] The Solid Project was established in 2015 as the first step to fix this. It aims to 'empower users and organisations by separating their data from the applications that use it'.[103] Should it happen, users would have full control over their data, and enjoy a new breed of applications 'with capabilities above and beyond anything that exists today'.[104] Inrupt is a commercial start-up established to protect 'the integrity and quality of the new web built on Solid'.[105] It sets up a number of founding principles, notably including 'Personal Empowerment through Data'.[106] Inrupt introduces its own version of PDS, the 'Personal Data Online Store' (POD), which would 'restore rightful ownership of data back to every web user...and unleash a new wave of innovation'.[107]

- *Data storage*: User data is stored in a POD, built on a Solid server.[108]

---

[97] HAT (n 94).
[98] ibid.
[99] ibid.
[100] ibid.
[101] The Evolution of Solid, available at <https://solid.inrupt.com/about>accessed 11 May 2019.
[102] Tim Berners-Lee, 'One Small Step for the Web' (The Medium, 29 September 2018) available at <https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085>accessed 11 May 2019.
[103] About Solid, available at <https://solid.inrupt.com/> accessed 11 May 2019.
[104] ibid.
[105] Berners-Lee (n 102).
[106] About Inrupt, available at <https://inrupt.com/>accessed 11 May 2019.
[107] ibid.
[108] Solid, 'Get a Solid POD and Identity', available at <https://solid.inrupt.com/get-a-solid-pod>accessed 12 May 2019.

- *Data access*: To note, the term Solid derives from 'Social Linked Data', a set of conventions and tools based on Linked Data principles. Therefore, Inrupt primarily relies on existing W3C standards and protocols and contains an API for building applications on Solid.[109]

## 11. Enigma (2015-)

The Enigma Project is a blockchain-based, peer-to-peer network that facilitates and secures a decentralised web.[110] Guy Zyskind, the CEO of Enigma, co-founded Enigma with Oz Nathan in 2015. They believe that something missing on the decentralised web,[111] that is, a privacy layer allowing multiple parties to jointly run applications over sensitive or private data while keeping them 'completely private'.[112] Once established, the decentralised web is, as Zyskind sees it, a 'black box' that process data inside and returns only the results.[113] They build this privacy layer using an advanced encryption technique called 'secure multi-party computation'.[114]

- *Data storage*: Enigma stores on a blockchain (what they call 'decentralised off-chain distributed hash-table') '*references* to the data and not the *data* themselves'.[115] Users should first encrypt their data so that data queries are computed in a distributed way, without a trusted third-party.
- *Data access*: Third-party services query off-chain data through the blockchain, which verifies the digital signature.[116]

[109] GitHub, Solid Project, available at <https://github.com/solid/solid>accessed 13 May 2019.
[110] About Enigma, available at <https://enigma.co/>accessed 11 May 2019.
[111] Enigma Project, 'Welcome to Enigma! Start Here' (The Medium, 5 November 2018) available at <https://blog.enigma.co/welcome-to-enigma-start-here-e65c8c9125ef>accessed 11 May 2019.
[112] ibid.
[113] Andy Greenberg, 'MIT's Bitcoin-inspired 'Enigma' Lets Computers Mine Encrypted Data' (WIRED, 30 June 2015) available at <https://www.wired.com/2015/06/mits-bitcoin-inspired-enigma-lets-computers-mine-encrypted-data/>accessed 11 May 2019.
[114] Overview of the Enigma Project, available at <https://www.media.mit.edu/projects/enigma/overview/>accessed 11 May 2019.
[115] Guy Zyskind, Oz Nathan and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy', available at <https://enigma.co/enigma_full.pdf>accessed 17 February 2019.
[116] ibid. See also Guy Zyskind, Oz Nathan and Alex Pentland, 'Decentralizing Privacy: Using Blockchain to Protect Personal Data'(2015 IEEE Security and Privacy Workshops, 21-22 May 2015, San Jose, CA, USA) 180, 181.

## 12. Databox (2016-19)

Databox is another EPSRC-funded, cross-University project to give individual control over the use of their data. Established in October 2016, this project aims to develop an open-source personal networked device (called 'databox'), within which data is kept safe and secure...and never given away'.[117] In a domestic IoT setting, a networked mini-computer is deployed to collate data from devices in the home and make them available to the apps in the Databox.[118] The developers derive the idea of databox from the GDPR, the advent of the Internet of Things (IoT), and the need to 'balance consumer concerns with commercial desire to exploit new opportunities'.[119]

- *Data storage*: the minicomputer (databox) collates, stores and exchange data within the box in IoT domestic setting. The processing of data is, as Urquhart and others explain, 'performed by the app, which runs locally on the box, thus eliminating the need for data to be sent to organisational servers'.[120]
- *Data access*: The databox enables controlled access to all data gathered into the box through APIs.[121] Haddadi and others reveal that this is achieved by making data 'selectively query-able so that users have fine-grained control over what data is made available to third parties'.[122] Urquhart adds that databox enables 'easy portability' *between* applications and services in the box.[123]

[117] HORIZON, What is Databox? available at <https://www.horizon.ac.uk/project/databox>accessed 11 May 2019.
[118] ibid.
[119] HORIZON, 'Why Databox' (HORIZON Blog, 28 November 2017) available at <https://www.horizon.ac.uk/why-databox/>accessed 11 May 2019.
[120] Urquhart and others (n 77) 324. See also Hamed Haddadi and others, 'Personal Data: Thinking Inside the Box' (2015) arXiv:1501.04737v1.
[121] ibid. See also Databox Developers, 'Fast and Simple Way to Deliver Your Data on Mobile', available at <https://developers.databox.com>accessed 13 May 2019.
[122] ibid.
[123] Urquhart and others (n 77) 324.

## IV. Data Trusts as an Alternative?

Indeed, these data trusts offer a varying degree of stewardship and collective management that are wanting in the case of UCTS. With these third parties stepping in, however, the use and reuse of personal data would be on the premise of aggregation of data from multiple sources and hence diverge from an individual's willingness to process data for his or her own good.

For instance, Open Data Institute (ODI) in the UK is one of the early pioneers facilitating data trusts in the UK. They set as the goal of their research project 'to increase access to data for new technologies while retaining trust'.[124] Three pilot studies are currently undergoing at the time of writing, respectively on the themes of IoT sensors/city public services, illegal wildlife trading and food waste.[125]

However, the ODI itself is unsure about the right form/infrastructure of data trusts and have spared efforts to explore all possible solutions. Hardinges points out that data trusts is a floating concept, and the term seems to cover 'a bundle of choices related to different aspects of data access'.[126]

The Government-commissioned report on AI seems to have revitalised this topic and bring it to the forefront of the AI. In this report, the two authors recommended a programme to develop Data Trusts in order to facilitate data access for AI development.[127] However, the notion of data trusts has been discussed for a long time, including narratives ranging from a B2B data-sharing agreement, third-party outsource management, government-endorsed initiatives and even regulation. In a B2B context, for instance, the notion of data trust is predominantly interpreted as a means to ascertain the IP rights

[124] For instance, see Jack Hardinges, 'What is a Data Trust?' (ODI Blog, 10 July 2018) <https://theodi.org/article/what-is-a-data-trust/>accessed 5 October 2019.
[125] ODI, 'Data Trusts: Lessons from Three Pilots (Report)' (ODI Blog, 15 April 2019) <https://theodi.org/article/odi-data-trusts-report/>accessed 5 October 2019.
[126] ibid.
[127] Dame Wendy Hall and Jérôme Pesenti, Growing the Artificial Intelligence Industry in the UK (UK Government-Commissioned Independent Report, 15 October 2017) https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

and associated benefits for the businesses concerned. While some of the data-sharing agreements speak to the solutions mitigating the risks of violating data subject rights, it remains questionable how this can be achieved without engagement of the individuals concerned. A somewhat better alternative to this involves an independent third party specialising in data management. Alex Blandford, ODI's Data Trust Policy Advisor, contends that the ODI favours, and hence put in, third party governance around data for a specific purpose.[128]

Alternatively, data trusts could be construed from the bottom. In a recent paper, Delacroix and Lawrence argued for bottom-up data trusts. In contrast to traditional approaches to pooling data, they contend that individuals could make most of the GDPR rights newly construed. Indeed, the GDPR rights themselves fall short of addressing the imbalance of power. To bring individual control out of a meaningless illusion and enable meaningful data reuse, GDPR rights have to be interfaced with management systems such as data trusts. In view of the difficulty in calling for a good number of individuals exercising these rights together, they suggest a pool of GDPR rights, i.e. the trustees (data trusts) exercise the GDPR rights for and on behalf of data subjects (trustors). Among other insights, the idea of data trusts is developed beyond, hence diverting from, previous discussions in the US by suggestion of trust pluralism. This suggestion is reasonably plausible as it aligns well with the data protection principle of purpose limitation. However, this GDPR-based approach to data trusts may be encountered with a number of challenges relating to the source and type of data being pooled. As argued previously, the issue of whether the portability rights given, DCD- and FFNPD-based data portability all taken into account, allow for the porting of aggregated data from incumbent controllers are contestable. As Wachter and others have argued, access and governance as such may require a new right to be established beyond the GDPR.[129] Even

[128] Alex Blandford, 'The ODI and Data Trusts: How Our Projects Will Work' (ODI Blog, 7 February 2019) <https://theodi.org/article/the-odi-and-data-trusts-how-our-projects-will-work/>accessed 5 October 2019.
[129] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019(2) Columbia Business Law Review 494-620.

full portability can be achieved, in the sense of machine-readability, these trusts could be facing pushbacks from other interested third parties as personal data is in nature relational and interpersonal.[130] Due to different sets of conditions and exceptions in the case of deleting data before porting them away might be unlikely to happen under the GDPR.[131] If the trusts suggested do not aim for a migration of data from the controller, perhaps they may adopt an API-based approach, currently promoted and tested in the UK. The whole idea of trusts may however be undermined as they are not in a position to decide and their legal status elusive.

In the realm of data trusts, there exists a wide variety of forms and structures relating to data access, reuse and control. Some data trusts appear to be commercial propositions that aim to increase consumer trust in the use of their personal data, and hence should be differentiated from the individual-centric ones, the UCTSes this chapter surveyed. Other trusts place third-party service provider, public bodies and even the government in the centre of stewardship, proposing city/civic trust or public oversight. In comparison, UCTSes attempt to manage and protect data for individuals while at the same time figuring out ways to capitalise on the use of data as part of their business models. The commercial nature of these intermediaries is the primary source of concerns, and perhaps the underlying reasons why they have not been fully trusted by users. Should we trust more on the non-profit third parties or even the governments, perhaps we can cast our eyes on the development of these data trusts. However, they could be facing sustainability challenges in terms of funding, governance and individual will. Departing from the commercial counterparts, these trusts are on the premise that an individual is unsuitable, or incapable of, becoming a steward for his or her personal data. Alternatively,

[130] Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict Between Right to Data Portability and Right to Be Forgotten under the General Data Protection Regulation' (2018) 8(4) International Data Privacy Law 309-317. See also Murray Goulden and others, 'Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT' (2018) 20(4) New Media & Society 1580–1599.
[131] See, for instance, Dominik Herrmann and Jens Lindemann, 'Obtaining Personal Data and Asking for Erasure: Do App Vendors and Website Owners Honour Your Privacy Rights' (2016) arXiv:1602.01804v2 [cs.CY].

we should seek stewardship from trust specialised third-parties. However, the whole idea of data trusts is already distinct from the original motive to create a right to data portability for an individual. In recent debates on data trusts, privacy and data protection law has been framed as a source of, rather than data itself, challenges to obtain data. For instance, a joint report by BPE, Pinsent Masons and Queen Mary University of London points to the requirements from the GDPR that have to be met by a trust.[132] Moreover, data trusts look beyond a collection of personal data of one individual and aim for data aggregation as its core. As Night rightly points out, 'data trusts work off the principle that an individual's data is worth very little, but in aggregate with enough others is worth a lot'.[133] Eventually, this seems to be a decision facing every data subject, between using data for personal interests, which we are now lacking a reliable method/solution, and contributing our data to a data trust and merge them with data of others, which perhaps not all of us have the motivation to do so. Perhaps data trusts would play a critical role, as an intermediary between different data sources, in pooling data and coordinating different wills of the individuals concerned.

## V. Reflections and Conclusion: More Trustworthy Systems or *Déjà vu*?

| | Openness | Data Storage | Access/Portability |
|---|---|---|---|
| All Advantage (1999-2001/2006) | Proprietary | N/A | Passive monitoring |
| Lumeria (1999-N/A) | Proprietary | PDS | Unknown |
| Higgins (2008-) | Open source | PDS (cloud-based) | An interoperable infrastructure for external websites; machine-readable data (in RDF) for users. |
| P3P (2002-) | Open (W3C protocols and standards) | N/A | N/A |

[132] Chris Reed and others, 'Data Trusts: Legal and Governance Considerations' (ODI Innovation Programme/Innovate UK, April 2019) 8.
[133] Jim Knight, 'Take it on Trust' (The Medium, 31 December 2017) https://medium.com/@jimpknight/take-it-on-trust-beb25a4b4ffc

| | | | |
|---|---|---|---|
| Mydex (2007-) | Proprietary | N/A | API |
| ownCloud (2010-) | Open-source (the Server edition) | Self-hosted | API |
| Personal/Digi.me (2009/2017-) | Proprietary | PDS (cloud-based) | API |
| Locker Project (2012-) | Open source | Self-hosted (PC-based) | API/TeleHash Protocol |
| HAT (2013-) | Open source | Self-hosted | API; Data Plugs |
| Solid/Inrupt (2015-) | Open (W3C protocols and standards) | PDS | W3C Standards and Protocols; REST API |
| Enigma (2015-) | Proprietary | Blockchain-based peer-to-peer network | Blockchain |
| DataBox (2016-) | Open-source | PDS | API |

Table 6.1 A selection of user-centric technological systems and their attributes

This chapter surveys contemporary concepts and projects concerning the user-centric technological systems. Potentially representing the future of data management and protection, these systems would interface well with the legal rights in the EU that facilitate data flows.

This quest starts with the early attempts to help consumers negotiate with vendors on how their data is used. In the presence of asymmetries of power and information, this negotiation process is proved inefficient and ineffective. Efforts were made, with limited success, to improve infrastructure design or facilitate technological empowerment to put consumers in a better position to bargain.

In parallel, there is an emerging industry known as infomediaries, specialising in negotiating on behalf of consumers. Theoretically viable, this human-based model nevertheless failed owing to the profit-driven nature and the impotence to strike a proper balance between privacy and data sharing. In reality, many infomediaries seem to prioritise the use of data over data protection to maintain sustainable development. As Kang and others point out, infomediaries 'leverage technologies to decrease the costs of matchmaking between individual privacy preferences and third-party marketers'.[134] With the rise of infomediaries, Givens expresses the concern that infomediaries amass considerable information power by 'aggregating very rich personal files'.[135] Dix also notes that many infomediaries in the market were not as privacy-friendly as promoted.[136] These scholars rightly brought up the questions as to whom to trust and whether infomediaries are more trustworthy than the suveilling businesses.

[134] Kang and others (n 29) 837.
[135] 'Panel on Infomediaries and the Negotiated Privacy', in Mary Meernik and Barbara Glover, 'Computers, Freedom and Privacy 2000 Challenges the Assumptions: The Audiotaped Proceedings' (2000) 17(10) Library Hi Tech News 1, 8-9.
[136] Alexander Dix, 'Infomediaries and Negotiated Privacy Techniques' (The Tenth Conference on Computers, Freedom and Privacy, New York, 2000) 167.

At the turn of the century, the infomediary model was quickly replaced by automated solutions powered by user-centric technologies. The appeal of these intelligent machines is that they provide for data management completely under an individual's control so that he or she does not have to outsource it to third or fourth parties. Through years of development, user-centric technologies are shifting from business tools for better matchmaking to individual assistants for data management. Given that the use of personal data is virtually non-negotiable in the digital age, a growing body of technological systems are being built with the user in the centre with complete control over data. Compared to the early human-based model, user-centric systems are characterised with data ownership, control and reverse licensing, thereby doing a better job at balancing data protection and data utility. Further, the adoption of new technologies such as API, Blockchain and AI could strengthen controlled access and open the door for data-driven innovation.

Several legal rights examined earlier would play a critical role in pushing data into these user-centric systems, together with technological means (such as the 'data plugs' in the case of HAT). This joint effort of law and technology could provide for a technology-mediated 'data utopia' where our data is better managed or protected. That said, the operation of law and technology is interdependent from each other. Not all the technological systems are built to comply with the law, and the data obtained through the GDPR may be channelled elsewhere and used for other purposes. Nevertheless, user-centric systems represent a good place to store, manage and control our personal data. If they thrive in the market and keep their promises, individuals would have the option to leave the discredited, risk-intensive and organisation-centric ecosystem.

As shown previously, these new systems are confronted with problems of their own. As new entrants to the market, they are still struggling to increase the adoption rate and raise user awareness. The European Data Protection Supervisor points to the fact that most PIMSes find it challenging to penetrate

the markets 'dominated by services based on the business models and technical architectures where individuals are not in control of their data'.[137] Further, user-centric systems are in direct competition with popular services that significantly benefit from the network effect, user inertia and the asymmetries of information and power. Julian Ranger, the founder of Digi.me, expresses the classic chicken-and-egg problem his company is facing:[138]

*Users need to find enough utility in Digi.me so that they would download the app and connect it to an increasing number of personal data points; business, on the other hand, would develop on this platform only if they have access to enough users to make it worth their while.*

Ranger explains that the only way to attract users and businesses is to make Digi.me more useful while at the same time seeking business partnership.[139] Enigma is facing a similar issue that the system requires a great number of users to adopt before it can start working securely and efficiently.[140] To this end, the company creates an incentive scheme that a user gets a tiny amount of bitcoin if she requests a computation from the Enigma network.[141]

Apart from the competitiveness of the market, further support from the public authorities is necessary for these emerging models to develop. As the EDPS concludes in its study on PIMS, additional incentives are necessary for new data protection business models to thrive.[142] In this respect, codes of conduct and certification schemes are recommended 'as privileged instruments to give specific visibility and role to the PIMS'.[143] Further, the EDPS suggests public eGovernment services to accept PIMS as a source of data, thereby 'adding critical amass of the acceptance of PIMS'.[144] In a similar vein, Rubinstein

[137] EDPS (n 7) 13.
[138] O'Hear (n 88).
[139] ibid.
[140] Greenberg (n 113).
[141] ibid.
[142] EDPS (n 7) 13-15.
[143] ibid.
[144] ibid.

contends that regulators should encourage these business models by offering 'regulatory flexibility and reduced penalties'.[145]

The legal rights examined above are not just crucial for the scalability of user-centric systems. Eventually, the question of trust persists in the case of user-centric technological system. To become the 'data utopia', they have to take active measures to make the system user-centric, transparent, open and interoperable. It is demonstrated that not all projects surveyed offer the option to leave. Notably, Higgins offers data exports in a machine-readable format, and Digi.me enables data exchange between PIMSes through the TeleHash protocol. Apart from these, many other projects are keen on exploring ways to facilitate data inflows, but are silent or ambiguous on the issue of data outflows. In the case when a system does not support the user to leave with his or her data, those legal rights would still play a critical role in facilitating switching between user-centric systems.

[145] Rubinstein (n 36) 87.

# Conclusion

This thesis provides a detailed analysis of the new right to data portability in the EU General Data Protection Regulation (GDPR), looking at the right's contribution to data protection in particular. Conventionally, the protection of personal data is achieved through carefully designed restrictions on data collection, processing and exchange. In the EU legal order, data protection is also a precondition for personal data flows, and the two values are inherently linked. Against this backdrop, the right to data portability represents an unprecedented way of protecting our personal data. It barely exerts an impact on the undergoing processing of personal data by the data controller. Rather, the right makes the most of the non-rivalrous nature of personal data by creating multiple copies for all stakeholders in need. In addition, the right to data portability does not directly restrict the power of the data controller; it empowers the data subject with the ability to process personal data so that the imbalance of power can be gradually corrected. Unlike the existing rights directly and immediately serving the goal of data protection, the right to data portability is thus a qualified contributor. It is contingent on the emergent user-centric technologies, the enhanced connectivity between processing systems, as well as the data subject's digital literacy.

In previous chapters, this right has been examined through the socio-technological (chapters 1, 6), legal (chapters 2-4), and technical (chapters 5-6) lens. It is noted that there is an interesting, understated interaction between data protection and data portability. On the one hand, the right to data portability is a unique legal construct inherently associated with the goal of data protection, despite the potential to pursue other goals. On the other, the introduction of such a right poses challenges to long-standing assumptions of data protection. The rest of the Conclusion sheds some light on the right's elusive nature and then summarises the wider implications of this right for data protection and beyond.

In sum, the GDPR right to data portability carves out two paths towards data protection. First, it can be used to direct data into new, user-centric systems (surveyed in Chapter 6) for better protection and management. Nonetheless, particular caution should be given to this idealised case. These user-centric systems are still in their early stage, requiring more time to evolve. The extent to which new systems are more trustworthy than incumbent ones needs to be empirically examined. Second, enhanced data flows directed by data subjects would raise the awareness of data protection and, in the long run, foster a data-friendly culture. While the GDPR right itself is inherently limited in scope, there are new data portability regimes in other areas of law devised to complement the GDPR. When used together, they have the potential to facilitate switching, alleviate lock-in, and eventually cultivate an individual-centric and –friendly ecosystem. That said, it should be kept in mind that the GDPR right is heavily fettered by technical, technological and legal preconditions. The right's impact on data protection is incremental, contingent upon the rise of data activism, and mediated by technology.

In achieving these goals, the right to data portability should not be viewed in isolation. In sum, the right interacts with other areas of law as well as technology at three levels. First, the new GDPR right complements and interacts with other rights in the EU data protection regime. Second, in the areas of consumer protection and competition law, there are new data portability schemes recently introduced that supplement the GDPR right. Third, the right to data portability connects well to the emergent user-centric technological systems, which provide ostensibly better solutions to data management but struggle to encourage data inflows.

In each of these contexts, the creation of the new GDPR right prompts us to rethink existing assumptions of data protection. With data portability at play, it is high time to reflect upon the objectives and instruments of data protection, the interplay between data protection and other interrelated areas of law and,

more broadly, the relationship between law and technology. Building upon previous chapters, the rest of this thesis address these issues below.

## I. Thinking Inside Data Protection Law

The association between data protection and data portability poses challenges to three fundamental assumptions about data protection law. First, data protection used to have a one-way impact on personal data flows. With data portability at play, the objective of the free flow of personal data now has a direct contribution to and, as a result, a growing impact on data protection. Second, the notion of individual control over personal data used to be understood primarily in a protective context. This needs to be revisited when the right to data portability allows the data subject to download, transmit and reuse personal data. While the majority of the existing rights support a form of control for data protection (*rectificatory control*), the new right to data portability represents a distinct form of control for data reuse (*redistributive control*). Third, the right to data portability is devised, similar to other existing rights, to micro-manage the process of data processing. It therefore needs to be used in conjunction with other rights strategically and holistically. These three observations are detailed below.

As illustrated in Chapters 2 -3, EU data protection law is not purely protective by nature. Apart from the goal of data protection, this area of law facilitates the free movement of personal data in the European Union. From the old Directive to the new Regulation, these two objectives, data protection and free movement of data, remain valid despite terminological modifications.[1] That

[1] In the GDPR, all references once made in the Directive to the right to privacy are all replaced by the right to protection of personal data, in consistency with Art 8 of the EU Charter of Fundamental Rights. 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 OJ L 281, 23.11.1995, p. 31–50, Art 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) OJ L 119, 4.5.2016, p. 1–88, Art 1. Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271, Art 8.

said, the interplay between the two, as well as the instruments for achieving them, should be revisited in the light of data portability.

Traditionally, all data protection rules contributed directly to the objective of data protection. The economic objective, on the other hand, was indirectly ensured by the consistent application of data protection rules across the EU. The GDPR right to data portability is distinct from other subject rights in contributing to the goals of data protection law. It aligns naturally with the economic objective and has an immediate impact on the free flow of personal data. Against this backdrop, the objective of free movement of personal data is no longer passively *ensured* in the up-to-date data protection regime. The new right to data portability now directly facilitates data flows across systems and, intermittently, across geographical borders. That said, the new right cannot be justified purely on economic grounds, due to its intrinsic association with data protection. As the increased data flows might, in the long run, have a positive impact on data protection, the two objectives of data protection law could be achieved in reverse order, a scenario beyond a literal reading of Art 1 GDPR.

Apart from two fundamental objectives, the normative preference of EU data protection law - *i.e.* enhanced individual control over personal data - has been diversified by the introduction of a new data portability right. Conventional rights devised to rectify, restrict, block and terminate the process of data processing fit well into the narrative of privacy-as-control. As a result, the EU notion of control was predominantly understood in relation to the dignitary aspect of individual welfare. With data portability in place, this dignity-based conception merits a re-assessment. To borrow Aristotle's idea about justice, existing rights are useful mainly for *rectificatory* purposes, the new right additionally exerts a *redistributive* impact on personal data flows.[2] In recognition of this added value, the concept of control should be partially decoupled from human dignity, thereby extending to the realm of free

[2] Aristotle, *The Nicomachean Ethics* (David Ross tr, OUP 2009) 86.

development of personality. That said, the GDPR right to data portability may still serve a rectificatory goal, especially when used in tandem with user-centric technologies. Further, the right's legitimacy of sitting in the data protection framework is deeply rooted in this rectificatory contribution. When used for economic benefits only, for instance, the right is unlikely to acquire legal status as a component of data protection or even giving expression to the fundamental right to data protection.

In essence, the right to data portability is one of the 'micro-rights' devised to micro-manage the processing of personal data. It exerts a specific impact on the process of processing, ostensibly in parallel with other micro-rights.[3] In due recognition of this attribute, it is argued that strategies should be developed for enforcing data protection rights in a holistic and strategic manner. Indeed, some preliminary strategies are developed in Chapter 2, regarding the combined use of Arts 15 (right of access), 17 (right to erasure) and 20 (right to be forgotten). Notably, the rights of access and to data portability can be used in a mutually reinforcing way. As a natural companion to them, the right to erasure might be used to remove the residual in the incumbent system when the porting of data is accomplished. Further to this, guidelines should be provided by data protection authorities, not just for data controllers to comply with the law, but more importantly, for data subjects to enforce their data protection rights. As will be shown shortly, these guidelines should extend beyond the scope of data protection since supplementary schemes do exist in interrelated areas of law.

The effective use of rights is just one side of the coin. As Blume puts it, despite the increased level of subject empowerment, data controllers are still playing

[3] There are exceptions where subject rights can be used in a conflictual manner, either by one or a number of data subjects. For instance, the exercise of the right to erasure (art 17 GDPR) would prevent the further request of subject access (art 15 GDPR) or data portability (art 20). With regard to the conflict between multiple data subjects, see Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict Between Right to Data Portability and Right to Be Forgotten under the General Data Protection Regulation' (2018) 8(4) International Data Privacy Law 309.

a leading role in both data processing and data protection.[4] The fact that the GDPR is a right-based scheme should not distract us from the critical role of data controllers in making these rights happen. Individual control over personal data should not be equated with putting individuals in a position to self-manage the risks associated with data processing. To a large extent, the implementation of GDPR rights depends upon a high level of transparency, accountability, data protection by design (in the sense of enforcing data protection rights) and open infrastructure.

## II. An External Face: Contemplating the Interaction of Data Protection Rights with Other Areas of Law

As shown in the beginning of the thesis, data portability has been sought for many of its normative values. The right to data portability is, however, a unique legal construct inherently associated with data protection. While tethered in the data protection framework, this right has enormous externalities that should be never underestimated. The right's interaction with many other areas of law determines, to a great extent, the contribution to data protection. For instance, the supplementary schemes introduced in the framework of Free Flow of Personal Data as well as in the Digital Content Directive are necessary to ensure that the personal data, when transmitted to better, more protective systems, can be reliably reused. Further, the applicability of information rights to personal data generates legal uncertainties concerning the implementation of the right to data portability. Last, the lessons drawn from the public sector are useful but special care should be taken to avoid new problems. This section summarises the interaction between the GDPR right and three other sets of EU rules, concerning (1) consumer protection and competition law (2) intellectual property rights, trade secrets and protection of databases and (3) the European Interoperability Framework.

[4] Peter Blume, 'The Inherent Contradictions in Data Protection Law' 2(1) International Data Privacy Law 26, 28.

Without data portability, the EU data protection regime used to be heavily grounded on the protection of human dignity. As Chapter 3 reveals, EU rules on data protection, consumer protection and competition law interact in such a way that data protection safeguards human dignity whereas consumer protection and competition law jointly promote consumer welfare. When new data portability schemes are created in each of these regimes, this trio of EU law deserves a re-evaluation.

Obviously, the GDPR stands in a central position in this evolving landscape. On the one hand, it represents a holistic approach to data protection and, as a result, the rights created ostensibly apply to all sectors. On the other, personal data flows are intrinsically associated with the objective of data protection, but new schemes have been created that supplement the GDPR to facilitate normative goals beyond data protection. As shown in Chapter 3, the Commission initially framed the GDPR right to data portability broadly as a means of switching. However, the final version of the GDPR abandoned this approach, adding many constraints to the new right on the grounds of data protection. The data portability right by itself is hence incapable of facilitating switching or freeing consumers from lock-in. By allowing for the porting of just *one copy of* personal data, the right appears to be a tool more suitable for multi-homing rather than for switching.

The ongoing convergence of EU law establishes a basis for arguing that the right to data portability may legitimately pursue goals other than data protection. In contrast to the issue of recognition of data protection in the competition analysis, the GDPR right's implications for consumer welfare is relatively understated. The FFNPD framework has already come into effect since November 2018, and the DCD should be transposed into domestic law by 2021. Parts of the framework promote the portability of non-personal data for a competitive data economy, and parts of the Directive facilitate the same for consumer welfare with regard to the supply of digital content and/or services. When used together with these supplementary schemes, the GDPR now has

the potential to facilitate switching or alleviating lock-in. It should be noted that the intended impact on consumer welfare or competition is not achieved by aligning the GDPR right with the logic of competition law, as many scholars advocate. Rather, the GDPR right may be used in conjunction with other schemes to facilitate switching or alleviate lock-in, while having the potential to protect personal data in tandem with user-centric technologies.

The growing tension between data protection and information rights is likely to lessen the impact of the right to data portability or restrict the scope of the data concerned. It remains to be seen whether copyright, trade secrets, *sui generis* right, and the free flow of non-personal data are legitimate reasons for refusing to provide data portability in full. Suffice to say, the balancing between the right to data portability and information rights largely depends upon what the former right is used for. The issue of whether the GDPR right can 'represent' data protection or acquire the status of a fundamental right should be assessed on an *ad hoc* basis.

To note, data taxonomies have been often used to distinguish several categories of data to which different sets of rules respectively apply. This taxonomy-based approach is, however, often too simplistic to acknowledge the technical complexities of data portability, as well as the intrinsic interaction of legal rules. For instance, the division between personal and non-personal data does not reflect, as the Commission acknowledges, the existence of mixed datasets containing both types of data inextricably linked with each other.[5] In this respect, the Commission's Guidance appears to prioritise GDPR over FFNPD because that separating of the dataset 'significantly decreases the value of the dataset' and that there is no such obligation in either framework.[6] When it comes to observed data, grey areas do exist, as shown in Chapter 4, where conflicting rights are applicable at the same time. This is

[5] European Commission, 'Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union', COM(2019) 250 final, pp. 4-10.
[6] ibid.

mostly a dilemma caused by the A29WP Guidelines with an overstretch of GDPR provisions.[7] As additional data (*e.g.* metadata) necessary for data transmission reuse can and should now be obtained via new schemes, in which balancing rules are developed,[8] it is suggested that the European Data European Data Protection Board, now in the role of the Article 29 Working Party,[9] should refine the EU guidelines when possible. More generally, as grey areas cannot be entirely removed, the taxonomy-based approach to data governance should be treated with special caution. In its stead, the prime focus should be put on the development of rules concerning how the rights should be balanced in conflict.

Data flows in the direction from organisations to individuals used to be rare in the EU legal order. As a result, data protection authorities are keen on drawing lessons from the public sector, where there already exists a set of concepts, standards, protocols, principles, recommendations for the delivery of public service.[10] Indeed, some universally transferable principles developed in the public sector would accelerate the development of technical infrastructures for data flows in the private counterpart. However, disparities do exist between the two spheres regarding when, how, and why data flows between organisations to individuals. Notably, public authorities have the resources to promote the goals of openness, inclusivity, reusability, among others; the same is not always true for businesses, especially the small- and medium-sized enterprises (SMEs).[11] In this respect, principles such as technology neutrality and proportionality should be duly respected to minimise the

[7] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 9-10.
[8] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services (Digital Content Directive), OJ L 136, 22.5.2019, p. 1–27, Art 16(4).
[9] European Data Protection Board, 'Endorsement 1/2018 of GDPR 29WP Guidelines' (EDPB, 25 May 2018) available at<https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en>accessed 26 November 2018.
[10] European Commission, *New European Interoperability Framework: Promoting Seamless Service and Data Flows for European Public Administrations* (Publications Office of the European Union, 2017).
[11] ibid 11-16.

negative impact of path dependency and ensure that SMEs are not burdened with excessive responsibilities in particular.

## III. Inspecting the Relationship between Law and Technology

The right to data portability is by nature a highly technical right. On the one hand, it would take time for data controllers to satisfy the specifications prescribed in the GDPR. On the other, it is an incremental process that the new technological systems build reliable interfaces with the legal rights and provide better solutions to data management. In either case, technologies play a crucial role in mediating data transmission, protection and reuse. Currently, both standards for interoperability and technological preconditions for user-centric management are being developed. Before these technical and technological conditions are met, the right to data portability cannot make a solid contribution to data protection.

To be fair, the right to data portability can be used in two primary ways. First, it is a useful tool for switching to cheaper, better, more innovative and privacy-friendly services. On the other, the right can be used to direct data into user-centric systems in which our personal data is supposedly better protected and managed. The two use cases resemble the double-helix structure found in the DNA – that is, two strands that wind around each other like a twisted ladder – and one's achievement or failure has an impact on the other. In the short term, individuals may have to make strategic choices between reuse/innovation and control/protection. When new systems come to their maturity, individuals may be provided with the user-centric management for both cases. As Westin envisioned in the 1960s:

*Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives*.[12]

[12] Alan Westin, *Privacy and Freedom* (The Bodley Head 1967) 7.

Before this data utopia comes, all stakeholders are confronted with considerable uncertainties. Businesses are testing the water in the ever-evolving legal landscape while awaiting guidelines for compliance. Individuals are equipped with more rights but may not fully understand which right is useful for what purpose. New technological systems are struggling to compete with incumbent ones, and their success depends mainly upon the enforcement of rules and policies. Apart from technical and technological endeavours, competent authorities are indeed in a critical role to alleviate the degree of uncertainties. As the GDPR has been transformed into a model that prioritises individual rights over paternalistic protection, it is crucial that data subjects are provided with sufficient guidance to use their rights effectively and that those user-centric systems are supported to provide necessary assistance to data activism.

Throughout history, technological advances have always prompted legislators and policy-makers to update their regulatory toolkits. Whereas technologies are ever-evolving, law often lags behind. The right to data portability seems to represent a reversal of this relationship between law and technology. From the standpoint of data reuse, the use of GDPR rights involves some risk-taking. Especially in the early implementation phase, the use of GDPR rights may lead to data insecurity, breach or even abuse.[13] The GDPR right is also forward-facing from the protection perspective. It is reasonable to believe that the GDPR right is cultivating a culture of data activism in which individuals are skilful, competent and tech-savvy. The right's contribution to data protection would start to be revealed when user-centric technologies are feasible, user-friendly, and competitive in the market.

[13] Janis Wong and Tristan Henderson, 'the Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR' (2019) International Data Privacy Law (forthcoming), DOI: 10.1093/idpl/ipz008. See also Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"' (SOUPS, August 11–13, 2019, Santa Clara, CA, USA).

## IV. Limitations and Future Research

With a focus on the link between data protection and data portability, this thesis is unable to deepen the discussions on data-driven innovation, data semantics, and the usefulness of user-centric technologies. Primarily engaging with legal rules at EU level, it does not cover derogations or restrictions that Member States make on the GDPR rights.[14]

Due to time limits, this thesis incorporates no empirical examination of the right to data portability or any other supplementary schemes. However, the mini-experiment made for this thesis, involving data portability requests to ten controllers, shows that the right's implementation could be a time-consuming and tedious process for both parties involved. Data subjects may have to engage with data controllers back and forth for authentication purposes but do not keep a record of all digital identities used. Data controllers may be unsure about the scope of data to be provided, and sometimes even confuse the new right with existing ones! At the time of writing, there existed few empirical investigations into the GDPR rights, not to mention the new right to data portability. However, the right's real effects can be examined only through empirical data. With due recognition of these important themes, this thesis leaves them for future research.

[14] For instance, the UK's Data Protection Act of 2018 substantially mirrors the GDPR but also entails exemptions from the right to data portability. Sec 24 states that the right does not apply to 'manual unstructured personal data held by the Freedom of Information (FOI) public authorities'. Parts 1-4 of the Schedule 2 detail the exemptions based on Art 6(2) and Art 23(1) GDPR, regarding crime and taxation, legal proceedings, functions designed to protect the public, audit functions and even certain functions of the Bank of England etc. Schedule 3 further excludes, under certain conditions, health data, social work data, education data and child abuse data from the scope of data portability. See Data Protection Act of 2018, c.12.

# Bibliography

## Case-law


Case C-5/08 Infopaq International [2009] ECR I-6569
Case C-7/97 Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and Others [1998] ECR I-7791
Case 27/76 United Brands Company and United Brands Continentaal BV v Commission of the European Communities [1978] ECR 207
C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECR I-11959
Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971
Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317
Case C-145/10 *Painer* [2011] ECR I-12533
C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU [2008] ECR I-00271
Case C-393/09 Bezpečnostní softwarová asociace - Svaz softwarové ochrany v Ministerstvo kultury [2010] ECR I-13971
Joined Cases C-403/08 Football Association Premier League Ltd and Others v QC Leisure and Others and C-429/08 Karen Murphy v Media Protection Services Ltd [2011] ECR I-09083C
Case C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG [2004] ECR I-05039
C-461/10 Bonnier Audio AB and Others v Perfect Communication Sweden AB ECLI:EU:C:2012:219
Case C-553/07, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer [2009] ECR I-03889
Case C-604/10 Football Dataco Ltd and Others v Yahoo! UK Ltd and Others ECLI:EU:C:2012:115
Case T-65/89 BPB Industries and British Gypsum v Commission [1993] ECR II-389
Joined Cases T-24/93 to T-26/93 and T-28/93 *Compagnie maritime belge transports and others v Commission* [1996] ECR II-1201
Case T-201/04 [2007] Microsoft Corp. v Commission of the European Communities [2007] ECR II-03601
Case T-203/01 Manufacture française des pneumatiques Michelin v Commission of the European Communities [2003] ECR II-04071
Case T-228/97 Irish Sugar plc v Commission of the European Communities [1999] ECR II-02969
Case No COMP/M.7217 - Facebook/WhatsApp


## Legislation

### *International Conventions*


Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 28.01.1981
Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final, 18.5.2018
Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018)2-final


### *EU Treaties and Charters*


Treaty on European Union (TEU), OJ C 326, 26.10.2012, p. 13–390
Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012, p. 47–390
Charter of Fundamental Rights of the European Union (CFR), OJ C 326, 26.10.2012, p. 391–407

*EU Directives*

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services (Digital Content Directive), OJ L 136, 22.5.2019, p. 1–27

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-how and Business Information (trade secrets) against their Unlawful Acquisition, Use and Disclosure (Trade Secrets Directive), OJ L 157, 15.6.2016, p. 1–18.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC (PSD2), OJ L 337, 23.12.2015, p. 35–127

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 (PSI2 Directive) OJ L 175, 27.6.2013, p. 1–8

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, OJ L 337, 18.12.2009

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC (PSD), OJ L 319, 5.12.2007

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-use of Public Sector Information (PSI Directive), OJ L 345, 31.12.2003, p. 90–96

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive), OJ L 108, 24.4.2002, p. 51–77

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases OJ L 77, 27.3.1996, p. 20–28

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 (Data Protection Directive), OJ L 281, 23.11.1995, p. 31–50.

*EU Regulations*

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union (FFNPD), OJ L 303, 28.11.2018

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ L 119, 4.5.2016, pp. 1–88

*EU Decisions*

Decision No 1926/2006/EC of the European Parliament and of the Council of 18 December 2006 Establishing a Programme of Community Action in the Field of Consumer Policy (2007-2013).

Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on Interoperability Solutions for European Public Administrations (ISA), OJ L 260, 03.10.2009

*Communications between EU Legislative Bodies*

European Commission, Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building A European Data Economy, SWD(2017) 2 final

European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union, COM(2017) 495 final
European Commission, Staff Working Document Impact Assessment Accompanying the Document - Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability between EU Information Systems (borders and visa) and Amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability between EU Information Systems (police and judicial cooperation, asylum and migration), SWD(2017) 473 final
European Commission, Proposal for A Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content (Proposal for the Digital Content Directive), COM(2015) 634 final
European Commission, Proposal for A Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods, COM(2015) 635 final
European Commission, Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, COM(2015) 192 final
European Commission, Staff Working Document Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, SWD(2015) 100 final
European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-driven Economy' COM(2014) 442 final
European Parliament Legislative Resolution on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), P7_TA(2014)0212, 12 March 2014
European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions -Against Lock-in: Building Open ICT Systems by Making Better Use of Standards in Public Procurement, COM (2013) 455 final
European Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (trade secrets) against their Unlawful Acquisition, Use and Disclosure, COM(2013) 813 final.
Jan Philipp Albrecht, Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Albrecht Report), A7-0402/2013, 21.11.2013
European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union, COM(2010) 609 final
European Commission, Commission of the European Communities, Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security COM(90) 314 final
European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012
European Commission, Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention,

Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, SEC(2012) 72 final

*United States*

The California Consumer Privacy Act (CCPA), AB-375
The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191
Customer Online Notification for Stopping Edge-Provider Network Transgressions (CONSENT) Act, 115th Congress, 2nd session, LEW18208

*United Kingdom*

The UK's Payment Services Regulations, 2017 No. 752
The UK's Communications Act, 2003 c. 21
Enterprise and Regulatory Reform Act, 2013 c. 24

*Brazil*

Brazilian General Data Protection Law, No. 13,709, 14.8.2018

## Books

Alan Westin, *Privacy and Freedom* (The Bodley Head 1967)
Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016)
Aristotle, *The Nicomachean Ethics* (David Ross tr, OUP 2009)
Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business School Press 1999)
Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (OUP 2008)
Claude Elwood Shannon, *The Mathematical Theory of Communication* (University of Illinois Press 1949)
David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Basic Books 1999)
David Weimer and Aidan Vining, *Policy Analysis: Concepts and Practice* (6th edn, Routledge 2017)
Doc Searls, *The Intention Economy: When Customers Take Charge* (Harvard Business Review Press 2012)
Eleni Kosta, *Consent in European Data Protection Law* (Brill 2013)
Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (HUP 2015)
Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing 2014)
Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (OUP 2014)
Herbert Kubicek, Ralf Cimander and Hans Jochen Scholl (eds), *Organisational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases* (Springer 2011)
Inge Graef, *Data as Essential Facility: Competition and Innovation on Online Platforms* (Kluwer Law International 2016)
John Hagel III and Mark Singer, *Net Worth: Shaping Markets When Customers Make the Rules* (Harvard Business School Press 1999)
John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books 2012)
Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (Yale University Press 2012)
Jürgen Bröhmer, Clauspeter Hill and Marc Spitzkatz (eds), *60 Years German Basic Law: The German Constitution and its Court - Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights* (Konrad-Adenauer-Stiftung e.V., 2012)
John Locke, *Two Treatises of Government* (first published in 1690, CUP 1988)
Lawrence Lessig, *Code 2.0* (Basic Books 2000)

Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 2000)
Lee Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014)
Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2016)
Nadezhda Purtova*, Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2012)
Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015)
Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014)
Sandeep Bhowmik, *Cloud Computing* (CUP 2017)
Rein Wesseling, *The Modernisation of EC Antitrust Law* (Hart Publishing 2000)
Richard Whish and David Bailey, *Competition Law* (7th edn, OUP 2012)
Rick Levine and others, *Cluetrain Manifesto: The End of Business as Usual* (Perseus Books 2001)
Roger Smith, *Property Law* (Longman 1996)
Sebastian Lohsse and others (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Hart Publishing 2017)
Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)
Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (Harper Collins 2000)
Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (HUP 2018).

## Articles

### *Journal Articles*

Adrien Alberini and Yaniv Benhamou, 'Data Portability and Interoperability: An Issue that Needs to be Anticipated in Today's IT-driven World' (2017) 8 Expert Focus 518
Alan Mitchell, Iain Henderson and Doc Searls, 'Reinventing Direct Marketing — With VRM Inside' (2008) 10(1) Journal of Direct Data and Digital Marketing Practice 3
Albertina Albors-Llorens, 'Competition and Consumer Law in the European Union: Evolution and Convergence' (2014) 33(1) Yearbook of European Law 163
Alfred C. Yen, 'Western Frontier or Feudal Society: Metaphors and Perceptions of Cyberspace' (2002)17 Berkeley Technology Law Journal 1207
Andrew Cormack, 'Is the Subject Access Right Now Too Great a Threat to Privacy?' (2016) 2(1) European Data Protection Law Review 15
Anita Allen, 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm' (2000) 32 Connecticut Law Review 86
Aris Ouksel and Amit Sheth, 'Semantic Interoperability in Global Information Systems: A Brief Introduction to the Research Area and the Special Section' (1999) 28(1) SIGMOD Record 5
Axel Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2
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 1
Barbara Engels, 'Data Portability Among Online Platforms' 5(2) Internet Policy Review 1
Bart Custers and Helena Uršič, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law 4
Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307
Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250
Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 475

Christophe Lazaro and Daniel Le Métayer, ‘Control over Personal Data: True Remedy or Fairy Tale?’ (2015) 12(1) SCRIPTed 3
Christopher Kuner and others, ‘When Two Worlds Collide: The Interface between Competition Law and Data Protection’ (2014) 4(4) International Data Privacy Law 247
Christopher Kuner, ‘Data Protection and Rights Protection on the Internet: the Promusicae Judgment of the European Court of Justice’ (2008) 30(5) European Intellectual Property Review 199
Christoph Enders, ‘The Right to Have Rights: The Concept of Human Dignity in German Basic Law (2010) 2(1) Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD) 1
Christopher Rees, ‘Tomorrow’s Privacy: Personal Information as Property’ (2013) 3(4) International Data Privacy Law 220
Claudia Diaz, Omer Tene and Seda Gürses, ‘Hero or Villain: The Data Controller in Privacy Law and Technologies’ (2013) 74 Ohio State Law Journal 923
Damian Clifford and Jef Ausloos, ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130
Daniel Solove, ‘Privacy Self-Management and the Consent Dilemma’ (2013) 126 Harvard Law Review 1880
Dana Petcu and Athanasios Vasilakos, ‘Portability in Clouds: Approaches and Research Opportunities’ (2014) 15(3) Scalable Computing: Practice and Experience 251
Edward J. Eberle, ‘The Right to Information Self-Determination’ (2001) 2001 Utah Law Review 965
Edward J. Eberle, ‘Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview’ (2012) 33(3) Liverpool Law Review 201
Eric Goldman, ‘A Coasean Analysis of Marketing’ (2006) 2006 Wisconsin Law Review 1151
Gabriela Zanfir, ‘The Right to Data Portability in the Context of the EU Data Protection Reform’ (2012) 2(3) International Data Privacy Law 149
Francisco Costa-cabral and Orla Lynskey, ‘Family Ties: The Intersection between Data Protection and Competition in EU Law’ (2017) 54 Common Market Law Review 11
Fred H. Cate and Viktor Mayer-Schönberger, ‘Tomorrow’s Privacy: Notice and Consent in a World of Big Data’ (2013) 3(2) International Data privacy Law 67
Gerrit Hornung and Christoph Schnabel, ‘Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination’ (2009) 25(1) Computer Law & Security Report 84
Gerrit Hornung and Christoph Schnabel, ‘Data Protection in Germany II: Recent Decisions on Online-searching of Computers, Automatic Number Plate Recognition and Data Retention’ (2009) 25 Computer Law & Security Review 115
Gianclaudio Malgieri, ‘“Ownership” of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?’ (2016) 20(5) Journal of Internet Law 2
Gianclaudio Malgieri, ‘User-provided Personal Content’ in the EU: Digital Currency between Data Protection and Intellectual Property’ (2018) 32(1) International Review of Law, Computers & Technology 118
Gloria González Fuster, ‘Balancing Intellectual Property Against Data Protection: A New Right’s Wavering Weight’ (2012) 14 IDP. Revista d'Internet, Dret i Política 34
Graham Greenleaf, ‘Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey’ (2017) 145 Privacy Laws & Business International Report 10.
Graham Greenleaf, ‘Renewing Convention 108: The CoE's “GDPR Lite” Initiatives’ (2016) 142 Privacy Laws & Business International Report 14
Graham Greenleaf, ‘Renewing Data Protection Convention 108: The COE’s “GDPR Lite” Initiatives’ (2016) 142 Privacy Laws & Business International Report 14
Gregory Keating, ‘Distributive and Corrective Justice in the Tort Law of Accidents’ (2000) 74 Southern California Law Review 193
Harri Kalimo and Klaudia Majcher, ‘The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace’ (2017) 42(2) European Law Review 210
Helena Uršič, ‘Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control’ (2018) 15(1) SCRIPTed 42

Inge Graef, Damian Clifford and Peggy Valcke, ‘Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law’ (2018) 8(3) International Data Privacy Law 200
Inge Greaf, Martin Husovec and Nadezhda Purtova, ‘Data Portability and Data Control: Lessons for an Emerging Concept in EU Law’ (2017) Tilburg Law School Research Paper No. 2017/22, available at <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3071875>accessed 18 October 2018.
Inge Graef, ‘Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union’ (2015) 39(6) Telecommunications Policy 502
Inge Graef, ‘How can Software Interoperability be achieved under European Competition Law and Related Regimes?’ (2014) 5(1) Journal of European Competition Law & Practice 6
Inge Graef and others, ‘Putting the Right to Data Portability into A Competition Law Perspective’ (2013) Law Journal of the Higher School of Economics 53
Ira Rubinstein, ‘Big Data: The End of Privacy or a New Beginning?’ (2013) 3(2) International Data Privacy Law 74
Ira Rubinstein, ‘Regulating Privacy by Design’ (2012) 26 Berkeley Technology Law Journal 1409
Jacob M. Victor, ‘The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy’ (2013) 123(2) Yale Law Journal 266
Janis Wong and Tristan Henderson, ‘the Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR’ (2019) International Data Privacy Law (forthcoming), DOI: 10.1093/idpl/ipz008.
Jef Ausloos and Pierre Dewitte, ‘Shattering One-way Mirrors – Data Subject Access Rights in Practice’ 8(1) International Data Privacy Law 4
Jerry Kang and others, ‘Self-Surveillance Privacy’ (2011) 97 Iowa Law Review 809
Jerry Kang and Benedikt Buchner, ‘Privacy in Atlantis’ (2004) 18(1) Harvard Journal of Law and Technology 229
J.C. Buitelaar, ‘Privacy: Back to the Roots’ (2012) 13(3) German Law Journal 171
Josef Drexl, ‘Designing Competitive Markets for Industrial Data: Between Propertisation and Access’ (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 257. Wolfgang Kerber, ‘Governance of Data: Exclusive Property vs. Access’ (2016) 47 International Review of Intellectual Property and Competition Law 759
Julie Cohen, ‘Examined Lives: Informational Privacy and the Subject as Object’ (2000) 52 Stanford Law Review 1373
Justin Hughes, ‘The Philosophy of Intellectual Property’ (1988) 77 Georgetown Law Journal 287
Kalinda Basho, ‘The Licensing of Our Personal Information: Is It a Solution to Internet Privacy’ (2000) 88 California Law Review 1507
Kenneth Laudon, ‘Markets and Privacy’ (1996) 39(9) Communications of the ACM 92
Kim Veltman, ‘Syntactic and Semantic Interoperability: New Approaches to Knowledge and the Semantic Web’ (2001) 7(1) New Review of Information Networking 159
Kiranbir Kaur, Sandeep Sharma and Karanjeet Singh Kahlon, ‘Interoperability and Portability Approaches in Inter-Connected Clouds: A Review’ (2017) 50(4) ACM Computing Surveys Art 49
Lawrence Lessig, ‘Privacy as Property’ (2002) 69(1) Social Research 247
Lawrence Lessig, ‘The Architecture of Privacy’(1999) 1 Vanderbilt Entertainment Law and Practice 56
Lee Bygrave, ‘Privacy Protection in a Global Context – A Comparative Overview’ (2004) 47 Scandinavian Studies in Law 319
Lachlan Urquhart, Neelima Sailaja and Derek McAuley, ‘Realising the Right to Data Portability for the Domestic Internet of Things’ (2018) 22 Personal and Ubiquitous Computing 317
Luke Stark and Anna Lauren Hoffmann, ‘Data Is the New What? Popular Metaphors and Professional Ethics in Emerging Data Culture’ (2019) Journal of Cultural Analytics (forthcoming)

Lilian Edwards and Michael Veale, ‘Slave to the Algorithm? Why A “Right to An Explanation” is Probably Not the Remedy You are Looking For’ (2017) 16(1) Duke Law and Technology Review 1
Lucio Scudiero, Bringing Your Data Everywhere: A Legal Reading of the Right to Portability (2017) 3 European Data Protection Law Review 119
Marc Rotenberg, ‘Fair Information Practices and the Architecture of Privacy’ (2001) 2001 Stanford Technology Law Review 1
Mary Meernik and Barbara Glover, ‘Computers, Freedom and Privacy 2000 Challenges the Assumptions: The Audiotaped Proceedings’(2000) 17(10) Library Hi Tech News 1
Michael Veale, Reuben Binns and Jef Ausloos, ‘When Data Protection By Design and Data Subject Rights Clash’ (2018) 8(2) International Data Privacy Law 105
Nadezhda Purtova, ‘The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10(1) Law, Innovation Technology 40
Nadezhda Purtova, ‘Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-determination off the Table, and Back on Again?’ (2014) 30(1) Computer Law & Security Review 6
Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, ‘The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law’ (2017) 54 Common Market Law Review 1427
Natalie Banta, ‘Property Interests in Digital Assets: The Rise of Digital Feudalism’ (2017) 38(3) Cardozo Law Review 1099
Neil Averitt and Robert Lande, ‘Using the ‘Consumer Choice’ Approach to Antitrust Law’ (2007) 74 Antitrust Law Journal 175
Neil Averitt and Robert Lande, ‘Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law’ (1997) 65(3) Antitrust Law Journal 713
Robert Carpenter, Walking from Cloud to Cloud: The Portability Issue in Cloud Computing 6(1) Washington Journal of Law, Technology & Arts 1
Omer Tene and Jules Polonetsky, ‘Big Data for All: Privacy and User Control in the Age of Analytics’ (2013) 11(5) Northwestern Journal of Technology and Intellectual Property 239
Omer Tene, ‘Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws’ (2013) 74(6) Ohio State Law Journal 1217
Orla Lynskey, ‘Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability’ (2017) 6 European Law Review 793
Paul Ohm, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2010) 57 UCLA Law Review 1701
Pamela Samuelson, ‘Privacy as Intellectual Property?’ (2000) 52(5) Stanford Law Review 1125
Pasquale Pagano, Leonardo Candela and Donatella Castelli, ‘Data Interoperability’ (2013) 12 Data Science Journal 19
Paul Quinn, ‘Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?’ (2018) 18(2) Global Jurist 81
Patricia Mell, ‘Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness’ (1996) 11 Berkeley Technology Law Journal 1
Paul Schwartz, ‘Property, Privacy, and Personal Data’ (2004) 117 Harvard Law Review 2055
Paul Schwartz, ‘Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices’ (2000) 2000(4) Wisconsin Law Review 743
Paul Schwartz, ‘The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination’ (1989) 37(4) American Journal of Comparative Law 675
Peter Benson, ‘The Basis of Corrective Justice and Its Relation to Distributive Justice’ (1992) 77(2) Iowa Law Review 515
Peter Blume, ‘The Inherent Contradictions in Data Protection Law’ (2012) 2(1) International Data Privacy Law 26
Peter Swire and Yianni Lagos, ‘Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique’ (2013) 72 Maryland Law Review 335
Peter Wegner, ‘Interoperability’ (1996) 28(1) ACM Computing Surveys 285
Pinar Akman, ‘“Consumer Welfare” and Article 82 EC: Practice and Rhetoric’ (2009) 32 World Competition Law and Economics Review 71

Rajiv Shah and Jay P. Kesan, ‘Lost in Translation: Interoperability Issues for Open Standards’ (2012) 8(1) I/S: A Journal of Law and Policy for the Information Society 119
Richard S. Murphy, ‘Property Rights in Personal Information: An Economic Defense of Privacy’ (1996) 84 Georgetown Law Journal 2381
René Mahieu and others, ‘Collectively Exercising the Right of Access: Individual Effort, Societal Effect’ (2018) 7(3) Internet Policy Review 1
Robert Bartlet, ‘Developments in the Law--The Law of Cyberspace’ (1999) 112 Harvard Law Review 1574
Sébastien J. Evrard, ‘Essential facilities in the European Union: Bronner and Beyond’ (2004) 10 Columbia Journal of European Law 491
Sascha Meinratht, James Losey and Victor Pickard, ‘Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide’ (2011) 19 CommLaw Conspectus 423
Shoshana Zuboff, ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30(1) Journal of Information Technology 75
Shyamkrishna Balganesh, ‘Quasi-Property: Like, but not Quite Property’ (2012) 160 University of Pennsylvania Law Review 1889
Susan Rose-Ackerman, ‘Inalienability and the Theory of Property Rights’ (1985) 85 Columbia Law Review 931
Stefano Barazza, ‘Commission v Microsoft: How to Set Reasonable Rates for Access to Interoperability Information and Evaluate their Innovative Character?’ (2013) 4(1) Journal of European Competition Law & Practice 55
Steven Hetcher, User-Generated Content and the Future of Copyright: Part One - Investiture of Ownership’ (2008) 10 Vanderbilt Journal of Entertainment and Technology Law 863
Steven Lorber, ‘Data Protection and Subject Access Requests’ (2004) 33 Industrial Law Journal 179
Tana Pistorius Pieter Koornhof, ‘Convergence Between Competition and Data Protection Law: A South African Perspective’ (2018) 8(3) International Data Privacy Law 277.
Thomas A. Burnham, Judy K. Frels and Vijay Mahajan, ‘Consumer Switching Costs: A Typology, Antecedents, and Consequences’ (2003) 31(109) Journal of the Academy of Marketing Science 109
Turgut Ayhan Beydoğan, ‘Interoperability-Centric Problems: New Challenges and Legal Solutions’ (2010) 18(4) International Journal of Law and Information Technology 301
Wenlong Li, ‘A Tale of Two Rights: Exploring the Potential Conflict between Right to data Portability and Right to Be Forgotten under the General Data Protection Regulation’ (2018) 8(4) International Data Privacy Law 309
Wolfgang Kerber and Heike Schweitzer, ‘Interoperability in the Digital Economy’ (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 39
Wolfgang Kerber, ‘Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection’ (2016) 11(11) Journal of Intellectual Property Law & Practice 856
Xavier Duncan L’Hoiry and Clive Norris, ‘The Honest Data Protection Officer’s Guide to Enable Citizens to Exercise their Subject Access Rights: Lessons from a Ten-Country European Study’ (2015) 5 International Data Privacy Law 190.
Zaw Z. Han and others, ‘Interoperability from Electronic Commerce to Litigation Using XML Rules’ (2007) 15(3) International Journal of Law and Information Technology 233

### *Contributions to the Edited Books*

Amit Sheth, ‘Changing Focus on Interoperability in Information Systems: From System, Syntax, Structure to Semantics’, in Michael Goodchild and others (eds.), *Interoperating Geographic Information Systems* (Kluwer Academic Publishers 1999) 5-29
Antoinette Rouvroy and Yves Poullet, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 45

Dana Petcu, ‘Portability and Interoperability between Clouds: Challenges and Case Study’ (2011), in Witold Abramowicz and others (ed.), *Towards a Service-based Internet* (Springer 2011) 62-74
Eleni Kamateri and others, ‘Cloud4SOA: A semantic-interoperability PaaS solution for multi-cloud platform management and portability’, in *European Conference on Service-Oriented and Cloud Computing* (Springer-Verlag 2013) 64-78
Fred H. Cate, ‘The Failure of Fair Information Practice Principles’ in Jane Winn (ed), *Consumer Protection in the Age of the Information Economy* (Routledge 2006) 341
Magdalena Kostoska, Marjan Gusev, and Sasko Ristov, ‘An Overview of Cloud Portability’, in Octavian Fratu, Nicolae Militaru, Simona Halunga (eds.), Future Access Enablers of Ubiquitous and Intelligent Infrastructures (Springer 2015) 248–254
Larry Korba and Steve Kenny, ‘Towards Meeting the Privacy Challenge: Adapting DRM’, in Joan Feigenbaum (ed), *Digital Rights Management* (Springer-Verlag Berlin Heidelberg 2003) 118-136
Livia Predoiu and Anna V. Zhdanova, ‘Semantic Web Languages and Ontologies’, in Mario Freire and Manuela Pereira (eds.), *Encyclopedia of Internet Technologies and Applications* (IGI Global 2007) 512-18
Masoud Hosseini and Brian E. Dixon, ‘Syntactic Interoperability and the Role of Standards’, in Brian E. Dixon (ed.), *Health Information Exchange: Navigating and Managing a Network of Health Information Systems* (2016) 123

### *Conference Papers*

Alexander Dix, ‘Infomediaries and Negotiated Privacy Techniques’ (The Tenth Conference on Computers, Freedom and Privacy, New York, 2000) 167
Elena Markoska, Ivan Chorbev, Sasko Ristov, and Marjan Gusev, ‘Cloud Portability Standardization Overview’ (MIPRO’15, Opatija, Croatia, 5-29 May 2015) 286–291
Fotis Gonidis, Iraklis Paraskakis, and Dimitri’s Kourtesis, ‘Addressing the Challenge of Application Portability in Cloud Platforms’ (SEERC’12, Thessaloniki, Greece, 24-5 September 2012)
Grace A. Lewis, ‘The Role of Standards in Cloud-computing Interoperability’ (HICSS '13, Washington D.C, USA, 7-10 January 2013) 1652–1661
Guy Zyskind, Oz Nathan and Alex Pentland, ‘Decentralizing Privacy: Using Blockchain to Protect Personal Data’ (2015 IEEE Security and Privacy Workshops, 21-22 May 2015, San Jose, CA, USA) 180-184
Janis Wong and Tristan Henderson, ‘How Portable is Portable? Exercising the GDPR’s Right to Data Portability’ (UbiComp/ISWC’18 Adjunct, 8–12 October 2018, Singapore)
Kostas Stravoskoufos and others, ‘A Survey on Approaches for Interoperability and Portability of Cloud Computing Services’ (CLOSER’14, Barcelona, Spain, 3-5 April 2014) 112-117.
Mariano Di Martino and others, ‘Personal Information Leakage by Abusing the GDPR “Right of Access”’ (SOUPS, August 11–13, 2019, Santa Clara, CA, USA)
Stefan Kolb and Guido Wirtz, ‘Towards Application Portability in Platform as a Service’ (SOSE ‘14, Washington D.C, USA, 7-11 April 2014) 218

*Online Papers and Reports*

Arvind Narayanan and others, 'A Critical Look at Decentralized Personal Data Architectures' (2012) arXiv:1202.4503v1 [cs.CY].
CtrlShift, ‘The New Personal Data Landscape’ (Ctrl-Shift, November 2011).
David Banisar, ‘The Right to Information and Privacy: Balancing Rights and Managing Conflicts’ (2011), World Bank Institute Governance Working Paper <http://dx.doi.org/10.2139/ssrn.1786473>accessed 7 August 2017
Deloitte, ‘Study on Emerging Issues of Data Ownership, Interoperability, (Re-)usability and Access to Data, and Liability’ (A Study prepared for the European Commission, SMART number 2016/0030, 2018)
Dominik Herrmann and Jens Lindemann, ‘Obtaining Personal Data and Asking for Erasure: Do App Vendors and Website Owners Honour your Privacy Rights?’ (2016) arXiv:1602.01804v2.

European Committee for Interoperable Systems, '"Cloud Switching" and the Free Flow of Data – Portability and Interoperability of Software and Data across Cloud Services' (ECIS Special Paper, 27 June 2016), available at<http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability>accessed 13 November 2018.
Gillian Whitworth and others, 'The EU General Data Protection Regulation: Opportunities for Grocery Retail' (Open Data Institute Whitepaper, 4 December 2017)
Guy Zyskind, Oz Nathan and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy', available at <https://enigma.co/enigma_full.pdf>accessed 17 February 2019.
Inge Graef and others, 'Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data' available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106791>accessed 10 May 2019
Inge Graef, Raphaël Gellert, Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (2018) TILEC Discussion Paper DP 2018-028
John Palfrey and Urs Gasser, 'Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation' (2008) Berkman Center Research Publication No. 2007-8
Lorrie Cranor and others, '2006 Privacy Policy Trends Report' (CyLab Privacy Interest Group, 31 January 2007)
Michael Veale, 'Data Management and Use: Case Studies of Technologies and Governance' (The Royal Society, 2018) available at <https://www.thebritishacademy.ac.uk/sites/default/files/Data%20Governance%20-%20Case%20studies.pdf>accessed 13 October 2018.
Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"' available at <https://marianodimartino.com/dimartino2019.pdf>accessed 5 June 2019.
Orla Lynskey, 'Regulating "Platform Power"' (2017) LSE Law, Society and Economy Working Papers 1/2017
Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (EDPS, 14 September 2015)
Yunfan Wang and Anuj Shah, 'Supporting Data Portability in the Cloud under the GDPR' (2017) available at <https://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf>accessed 28 November 2018

## Official Guidelines, Opinions and Reports

Article 29 Working Party, 'Opinion on Commission Proposals on Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa as well as Police and Judicial Cooperation, Asylum and Migration' (WP266, 11 April 2018)
Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017)
Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, 13 December 2016)
European Data Protection Supervisor, 'Opinion on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (Opinion 4/2017, 14 March 2017)
European Data Protection Supervisor, 'Opinion on Meeting the Challenges of Big Data: A Call for Transparency, User control, Data Protection by Design and Accountability (Opinion 7/2015, 19 November 2015)
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' (Preliminary Opinion, March 2014)
European Data Protection Supervisor, 'Towards Excellence in Data Protection' (Strategy 2013-2014, 22 January 2013)

European Data Protection Supervisor, ‘Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - “A comprehensive approach on personal data protection in the European Union”’ (EDPS Opinion, 14 January 2011)
European Commission, Communication from the Commission — Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings OJ C 45, 24.2.2009.
European Commission, ‘GDPR Data Portability and Core Vocabularies’ (ISA2 Programme, November 2018)
Information Commissioner’s Office, ‘Subject Access Code of Practice: Dealing with Requests from Individuals for Personal Information’ (version 1.2, 9 June 2017)
Information Commissioner’s Office, ‘Guide to the General Data Protection Regulation’ (ICO Data Protection, Version 1.0.248, 2 August 2018)

## Policy Papers

BIS, ‘Better Choices: Better Deals—Consumers Powering Growth’ (GOV.UK, 13 April 2011)
BIS, ‘midata: 2012 Review and Consultation’ (GOV.UK, 27 July 2012)
BIS, ‘Government Response to 2012 Consultation’ (GOV.UK, 27 July 2012)
BIS, ‘Enterprise and Regulatory Reform Act 2013: A Guide’ (GOV.UK, 10 June 2013)
BIS, ‘Enterprise & Regulatory Reform Bill – Midata’ (GOV.UK, BIS/13/656, February 2013)
BIS, ‘Switching Principles: Call for Evidence’ (GOV.UK, 22 October 2015)
BIS, ‘Switching Principles: Government Response and Action Plan’ (GOV.UK, May 2016)
BIS, ‘Modernising Consumer Markets: Consumer Green Paper’ (GOV.UK, 11 April 2018)
Cabinet Office, ‘Consumer Empowerment Strategy Published’ (GOV.UK, 13 April 2011) <https://www.gov.uk/government/news/consumer-empowerment-strategy-published>accessed 9 February 2018.
CMA, ‘Energy Market Investigation Summary of Provisional Findings Report’ (GOV.UK, 7 July 2015)
CMA, ‘Retail Banking Market Investigation: Provisional Decision on Remedies’ (GOV.UK, 17 May 2016)
CMA, ‘Retail Banking Market Investigation: Final Report’ (GOV.UK, 9 August 2016)
CMA, ‘Digital Comparison Tools Market Study: Final Report’ (GOV.UK, 27 September 2017)
DCMS and BEIS, ‘Policy Paper: Smart Data Review’ (GOV.UK, 28 September 2018)
DCMS, ‘UK Digital Strategy 2017 Policy Paper’ (GOV.UK, 1 March 2017)
European Commission, ‘EU Consumer Policy Strategy 2007-2013: Empowering Consumers, Enhancing Their Welfare, Effectively Protecting Them’ COM (2007) 99 final.
Financial Conduct Authority, ‘Implementation of the Revised Payment Services Directive (PSD2): Approach Document and Final Handbook Changes’ (Policy Statement PS17/19, September 2017)
House of Commons Science and Technology Committee, ‘The Big Data Dilemma’ (HC 468, 12 February 2016)
Independent Commission on Banking (ICB), ‘Independent Commission on Banking: Final Report’ (GOV.UK,12 September 2011)
National Science and Technology Council (NSTC), ‘A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future’ (White House Archive, June 2011)
OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 2013
OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information (C(2008)36, 30 April 2008)
OECD, ‘OECD Expert Workshop on Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-use’, (DSTI/CDEP/SPDE(2018)4, 19 April 2018)
OECD, Recommendation of the Council on Health Data Governance (OECD Legal Instruments, 13 December 2016)
OECD, ‘Expert Workshop on Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use’ (SPDE(2018)4, 19 April 2018)

OECD Working Party on Security and Privacy in the Digital Economy, 'Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking' (DSTI/ICCP/REG(2014)3, 20 May 2014)
Ofcom, 'Strategic Review of Consumer Switching: A Consultation on Switching Processes in the UK Communications Sector' (Ofcom Public Consultation, 10 September 2010)
Ofcom, 'General Conditions of Entitlement', (Unofficial Consolidated Version, 30 July 2018) B3. Ofcom, 'Strategic Review of Consumer Switching: A Consultation on Switching Processes in the UK Communications Sector' (10 September 2010)
Open Data Institute and Fingleton Associates, 'Data Sharing and Open Data for Banks: A Report for HM Treasury and Cabinet Office' (HM Treasury, September 2014)
Osborne Clarke LLP, 'Legal Study on Ownership and Access to Data' (Smart Number 2016/0085, 24 May 2016)
The Obama Administration, 'Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (The White House Office, February 2012)
World Economic Forum, 'A New Lens for Strengthening Trust' (Rethinking Personal Data Project, May 2014)
World Economic Forum, 'Personal Data: The Emergence of a New Asset Class' (Rethinking Personal Data Project, January 2011)

## Standards

European Commission, *New European Interoperability Framework: Promoting Seamless Service and Data Flows for European Public Administrations* (Publications Office of the European Union, 2017)
International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Cloud Computing - Interoperability and Portability', (ISO/IEC 19941:2017, 1st edn., 15 December 2017)
International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Cloud computing - Overview and Vocabulary', (ISO/IEC 17788:2014, 1st edn., October 2014)
International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Document Container File -- Part 1: Core', (ISO/IEC 21320-1:2015, 1st edn., October 2015)
International Organisation for Standardization/International Electrotechnical Commission, 'Information Technology - Open Virtualization Format (OVF) Specification', (ISO/IEC 17203:2017, 2nd edn., September 2015)

IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries 610 (IEEE 610-1990, 18 January 1991)
Data Transfer Project, 'Overview and Fundamentals' (DTP Whitepaper, 20 July 2018) available at < https://datatransferproject.dev/dtp-overview.pdf >accessed 9 May 2019.
Open Data Institute, 'Introducing Open Banking Standard: Helping Customers, Banks and Regulators Take Banking into A Truly 21st-Century, Connected Digital Economy' (ODI Whitepaper, 2016)

## Webpages

Adam Chernichaw, 'White House Re-Introduces Consumer Privacy Bill of Rights Act' (White & Case, 8 April 2015) available at <https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act>accessed 17 December 2018.
Alexander Macgillivray and Jay Shambaugh, 'Exploring Data Portability' (White House Archive, 30 September 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability>accessed 17 December 2018.
Alexander Macgillivray, 'Summary of Comments Received Regarding Data Portability' (White House Archive, 10 January 2017) available at

<https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability>accessed 17 December 2018.
Andrew Cormack, ‘Portability Right: A Data Protection Challenge’ (JISC Community, 19 April 2017) available at <https://community.jisc.ac.uk/blogs/regulatory-developments/article/portability-right-data-protection-challenge>accessed 25 May 2019.
Andy Greenberg, ‘MIT's Bitcoin-inspired 'Enigma' Lets Computers Mine Encrypted Data’ (WIRED, 30 June 2015) available at <https://www.wired.com/2015/06/mits-bitcoin-inspired-enigma-lets-computers-mine-encrypted-data/>accessed 11 May 2019
Aneesh Chopra, ‘Modelling a Green Energy Challenge after a Blue Button’ (White House Archive, 15 September 2011) available at <https://obamawhitehouse.archives.gov/blog/2011/09/15/modeling-green-energy-challenge-after-blue-button> accessed 17 December 2018.
Antonio García Martínez, ‘No, Data Is Not the New Oil’ (WIRED, 25 February 2019) available at <https://www.wired.com/story/no-data-is-not-the-new-oil/>accessed 14 May 2019.
Anthony Cuthbertson, 'Google+ to Shut Down Early after Data from 52 Million Users Exposed' (Independent, 11 December 2018) available at <https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-plus-shut-down-date-bug-personal-data-breach-alphabet-inc-a8677296.html>accessed 20 December 2018.
Aradhna Chetal and others, ‘Interoperability and Portability’ (Cloud Security Alliance Group 4, 22 August 2011) available at<https://cloudsecurityalliance.org/wp-content/uploads/2011/09/Domain-6.docx>accessed 25 November 2018.
Arjun Kharpal, ‘Facebook Rolled out Privacy Changes — but it’s Being Forced to Do it Anyway by Regulators’ (CNBC, 29 March 2019) available at<https://www.cnbc.com/2018/03/29/facebook-has-rolled-out-privacy-changes--but-its-doing-it-for-gdpr.html>accessed 14 May 2019
Apple, ‘This is How We Protect Your Privacy’ available at <https://www.apple.com/uk/privacy/approach-to-privacy/>accessed 8 May 2019.
‘Apple’s Commitment to Customer Privacy’ (16 June 2013) available at <https://www.apple.com/apples-commitment-to-customer-privacy>accessed 2 August 2018.
Bernadette Hyland and others, ‘Linked Data Glossary’ (W3C Working Group, 27 June 2013) available at <https://www.w3.org/TR/ld-glossary>accessed 4 December 2018.
Brian Fitzpatrick, ‘The Data Liberation Front Delivers Google Takeout’ (Data Liberation Blog, 28 June 2011) available at <http://dataliberation.blogspot.com/2011/06/data-liberation-front-delivers-google.html>accessed 20 December 2018.
Bruce Sterling, ‘The Ello Bill Of Rights for Social Network Users’ (WIRED, 7 January 2015) available at <https://www.wired.com/beyond-the-beyond/2015/07/ello-bill-rights-social-network-users>accessed 12 December 2018.
Bundeskartellamt, ‘Bundeskartellamt prohibits Facebook from combining user data from different sources’ (Bundeskartellamt News, 7 February 2019) available at<https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>accessed 7 May 2019.
Centre for Information Policy Leadership, ‘Comments on the Article 29 Data Protection Working Party’ s “Guidelines on the right to data portability Adopted on 13 December 2016’ (15 February 2017) available at<https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf>accessed 6 May 2019
Christina Gagnier and Gagnier Margossian, ‘A Social Network Users’ Bill of Rights: “You” Must Decide’ (2011) available at <https://www.w3.org/2011/track-privacy/papers/GagnierMargossian.pdf>accessed 16 December 2018.
Council of Europe, ‘Convention 108 and Protocols’, available at <https://www.coe.int/en/web/data-protection/convention108-and-protocol>accessed 17 February 2019.
CtrlShift, ‘Data Mobility: The Personal Data Portability Growth Opportunity for the UK Economy’ (A Report Prepared for the DCMS, 19 November 2018) available at <https://www.gov.uk/government/publications/research-on-data-portability>accessed 25 May 2019.

Crunchbase, Overview of the Data Portability Project, available at<https://www.crunchbase.com/organization/dataportability>accessed 16 December 2018.
'Data is the New Currency' (KPMG, 20 November 2018) available at <https://home.kpmg/im/en/home/insights/2018/11/data-is-the-new-currency.html>accessed 14 May 2019.
Data Portability Project, available at <http://www.dataportability.org>accessed 16 December 2018
Data Transfer Project, 'Overview and Fundamentals' (DTP Whitepaper, 20 July 2018) available at <https://datatransferproject.dev/dtp-overview.pdf>accessed 8 June 2019.
Data Transfer Project, 'About Us', available at <https://datatransferproject.dev>accessed 10 May 2019.
Data Transfer Project, 'Why Do We Need the Data Transfer Project', available at <https://datatransferproject.dev/why-dtp>accessed 20 December 2018.
Data Transfer Project, 'How Does DTP Work', available at <https://datatransferproject.dev/how-does-dtp-work>accessed 20 December 2018
Dessislava Savova and others, 'French Law for A Digital Republic Anticipating the Impact of the GDPR' (Talking Tech, 17 April 2017) available at <https://talkingtech.cliffordchance.com/en/data-cyber/data/french-law-for-a-digital-republic-.html>accessed 19 February 2019.
Duncan Work, 'Call for A Social Networking Bill of Rights' (Planetwork Journal, July 2004) available at <http://planetwork.net/journal>accessed 16 December 2018.
Ellen Tannam, 'Tech Titans Join Forces for the Data Transfer Project – so How Will it Work?' (Silicon Republic, 20 July 2018) available at <https://www.siliconrepublic.com/enterprise/data-transfer-project-explained>accessed 2 June 2019.
European Commission, 'Press Release - Security Union: Commission Closes information gaps to better protect EU citizens', (Press Release, 12 September 2017) available at <http://europa.eu/rapid/press-release_IP-17-5202_en.htm>accessed 10 November 2018.
European Commission, 'New Version of European Interoperability Reference Architecture available', (Digital Single Market, 4 September 2017) available at <https://ec.europa.eu/digital-single-market/en/news/new-version-european-interoperability-reference-architecture-available>accessed 10 November 2018.
European Commission, 'Frequently Asked Questions - Interoperability of EU Information Systems for Security, Border and Migration Management' (Factsheet, 12 December 2017), available at <http://europa.eu/rapid/press-release_MEMO-17-5241_en.htm>accessed 10 November 2018.
European Commission, 'Interoperability' (Digital Single Market Policy, 15 June 2018) <https://ec.europa.eu/digital-single-market/en/interoperability> accessed 10 November 2018.
European Commission, 'The New European Interoperability Framework' (ISA2, 9 May 2019) available at <https://ec.europa.eu/isa2/eif_en>accessed 9 May 2019.
European Commission, 'Building a European Data Economy' (Digital Single Market Policy, 24 January 2019) available at<https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>accessed 9 August 2018
European Commission, 'Payment Services Directive: Frequently Asked Questions' (Factsheet, 12 January 2018) available at <http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm>accessed 21 December 2018.
European Commission, 'Factsheet on the "Right to Be Forgotten" Ruling (C-131/12), available at<https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf>accessed 29 March 2019
Emily Bater, 'Midata - Making Comparison Better' (GoCompare) available at <https://www.gocompare.com/money/midata>accessed 22 December 2018.
'Facebook – Bundeskartellamt's Landmark Decision Blurs the Line between Data Protection and

Competition Law (Linklaters, 28 February 2019) available at<https://www.linklaters.com/en/insights/publications/2019/april/facebook-bundeskartellamt-s-landmark-decision>accessed 7 May 2019.
Google Account, 'Download Your Data' available at <https://takeout.google.com/settings/takeout>accessed 20 December 2018.
HAT, 'Introducing the Hub-of-All-Things (HAT) and the HAT Ecosystem', available at <https://static1.squarespace.com/static/5b5988f9b105985261c0a722/t/5c179df3f950b7d4a378c11b/1545051654456/hatpresentation1.7PDF.pdf>accessed 12 May 2019
Health Information Privacy Division, 'Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524' (HHS.GOV, 5 February 2016) available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs>accessed 22 December 2018
HHS, 'Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules' (Office of the Federal Register, 25 January 2013) available at <https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>accessd 10 May 2019.
HM Treasury and The Rt Hon George Osborne, 'Bank Account Switching Service Set to Launch' (GOV.UK, 10 September 2013) available at <https://www.gov.uk/government/news/bank-account-switching-service-set-to-launch>accessed 22 December 2018.
HORIZON, 'Why Databox' (HORIZON Blog, 28 November 2017) available at <https://www.horizon.ac.uk/why-databox/>accessed 11 May 2019
Hunton Andrews Kurth, 'DPA of Argentina Issues Draft Data Protection Bill' (Privacy & Information Security Law Blog, 9 February 2017) available at <https://www.huntonprivacyblog.com/2017/02/09/dpa-argentina-issues-draft-data-protection-bill>accessed 19 February 2019.
Jack Lerner and Lisa Borodkin, 'We, the Users - Facebook Users' Bill of Rights' (SF Gate, 21 May 2010) available at <https://www.sfgate.com/opinion/article/We-the-users-Facebook-users-Bill-of-Rights-3263476.php>accessed 16 December 2018.
Jack Hardinges, 'Will GDPR and Data Portability Support Innovation?' (ODI, 15 February 2018) available at <https://theodi.org/article/will-gdpr-and-data-portability-support-innovation/>accessed 25 May 2019.
James Denvil and Patrick Kane, 'Insights on the Consumer Privacy Bill of Rights Act of 2015' (Hogan Lovells Chronicle of Data Protection, 3 March 2015) available at <https://www.hldataprotection.com/2015/03/articles/consumer-privacy/insights-on-the-consumer-privacy-bill-of-rights-act-of-2015>accessed 17 December 2018.
Jeff Jarvis. 'My Cyberspace Bill of Rights' (The Guardian, 29 March 2010) available at <https://www.theguardian.com/commentisfree/2010/mar/29/internet-censorship-cyberspace-bill-of-rights >accessed 16 December 2018.
Jon Porter, 'GDPR Makes it Easier to Get Your Data, but that Does Not Mean You Will Understand it: 138 GB of data and No Real Answers' (The Verge, 27 January 2019) available at <https://www.theverge.com/2019/1/27/18195630/gdpr-right-of-access-data-download-facebook-google-amazon-apple>accessed 14 May 2019.
John Battelle, 'The Data Bill of Rights' (Battelle Media, 25 April 2007) available at <https://battellemedia.com/archives/2007/04/the_data_bill_of_rights>accessed 16 December 2018.
Joseph Smarr and others, 'A Bill of Rights for Users of the Social Web' (Open Social Web, September 2007) available at <https://domainmarketresearch.com/?page_id=359>accessed 16 December 2018.
Josh Constine, 'Friend Portability is the Must-have Facebook Regulation' (TechCrunch, 12 May 2019) available at <https://techcrunch.com/2019/05/12/friends-wherever/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=2XPb9v3gGAI50uJ77kTKTw>accessed 14 May 2019.
Letter from Facebook User Operations (Data Access Request Team) to Max Schrems, 28 September 2011, available at <http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf>accessed 8 May 2019.

Kaitlyn Tiffany, ‘Angry Birds and the End of Privacy’ (Vox, 14 May 2019) available at <https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush>accessed 3 June 2019
KCL Research Data Management, ‘Research Data Metadata: A Short Glossary of Basic Terms and Definitions’ (Library Services User Guide, 25 May 2015), available at <https://www.kcl.ac.uk/library/researchsupport/research-data-management/metadata-glossary.pdf>accessed 6 December 2018.
Kristen Honey, Phaedra Chrousos, and Tom Black, ‘My Data: Empowering All Americans with Personal Data Access’ (White House Archive, 15 March 2016) available at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access>accessed 17 December 2018.
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 16 December 2018.
Mark Sullivan, ‘A Bill of Rights for Facebook Users’ (PC World, 20 May 2010) available at <https://www.pcworld.com/article/196798/BOR.html>accessed 16 December 2018.
Natarajan Chandrasekaran, ‘Is Data the New Currency?’ (WEF Agenda, 14 August 2015) available at < https://www.weforum.org/agenda/2015/08/is-data-the-new-currency/>accessed 14 May 2019.
Office for Civil Rights (OCR), ‘Summary of the HIPAA Privacy Rule’ (HHS.GOV, 26 July 2013) available at <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>accessed 22 December 2018.
Olivier Proust and Gaëtan Goossens, ‘France Adopts Digital Republic Law’ (Fieldfisher Privacy Law Blog, 4 October 2016) available at <https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law>accessed 19 February 2019.
Open Banking Working Group, ‘The Open Banking Standard: Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation’ (Open Data Institute, 8 February 2016) available at <https://www.scribd.com/doc/298569302/The-Open-Banking-Standard>accessed 21 December 2018.
Open Banking, available at<https://www.openbanking.org.uk>accessed 21 December 2018.
Open Data Handbook: Glossary, available at <http://opendatahandbook.org/glossary/en>accessed 22 December 2018.
Overview of the Enigma Project, available at <https://www.media.mit.edu/projects/enigma/overview/>accessed 11 May 2019
Steve O’Hear, ‘Digi.me and Personal Merge to Put You in Control of the Nascent “Personal Data Ecosystem”’ (TechCrunch, 17 August 2017) available at <https://techcrunch.com/2017/08/17/digi-me-and-personal-merge/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=vasf1c48PqL5o27_wN2YGg>accessed 11 May 2019.
Personal Data Ecosystem Consortium, ‘Members of the PDEC Startup Circle’, available at <http://pde.cc/startup-circle/#2011>accessed 11 May 2019.
Phil Libin, ‘Evernote’s Three Laws of Data Protection’ (Evernote Blog, 3 June 2014) available at <https://evernote.com/blog/three-laws-of-data-protection-update>accessed 20 December 2018.
Parker Higgins, ‘Mobile User Privacy Bill of Rights’ (EFF, 2 March 2012) available at <https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights>accessed 16 December 2018.
Paul Bischoff, ‘What is the Consumer Privacy Bill of Rights?’ (CompariTech, 27 November 2018) available at <https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/>accessed 5 May 2019.
Peter Hustinx, ‘Data Protection and Competition: Interfaces and Interaction’ (Seminar Covington & Burling LLP, Brussels, 13 June 2013) available at <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/data-protection-and-competition-interfaces_en>accessed 8 May 2019.
Renato Leite Monteiro, ‘The New Brazilian General Data Protection Law — A Detailed Analysis’ (IAPP, 15 August 2018) available at <https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>accessed 4 May 2019.

Ro Khanna, Internet Bill of Rights, available at <https://www.rokhanna.com/issues/internet-bill-rights>10 May 2019.
Sara Ashley O'Brien, 'I Downloaded 14 Years of my Facebook Data and Here's What Happened' (CNN, 25 March 2018) available at <https://money.cnn.com/2018/03/24/technology/facebook-data/index.html>accessed 6 May 2019
Scott Carey, 'How Google Decides to Open Source its Technology: Two Google Executives Shine a Light on the Tech Giant's Open Source Strategy' (Computer World, 6 August 2018) available at <https://www.computerworld.com.au/article/644791/how-google-decides-open-source-its-technology/ >accessed 2 June 2019.
'Symposium on Data Protection and Competition Law' (International Data Privacy Law, August 2018) available at <https://academic.oup.com/idpl/issue/8/3>accessed 7 June 2019.
'The MyStudentData Download Function Allows You to Access Your Federal Student Aid Information or Your FAFSA Information in A Plain Text File', available at <https://studentaid.ed.gov/sa/resources/mystudentdata-download#what-is-mystudentdata>accessed 17 December 2018.
The World's Most Valuable Resource is No Longer Oil, but Data' (The Economist, 6 May 2017) available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>accessed 14 May 2019.
The White House Office of the Press Secretary, 'We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online' (White House Archive, 23 February 2012) available at <https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>accessed 16 December 2018
The EU glossary, available at<http://eur-lex.europa.eu/eli-register/glossary.html>accessed 6 December 2018.
The OECD Privacy Framework (2013), available at <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>accessed 9 May 2019
Tim Berners-Lee, 'One Small Step for the Web' (The Medium, 29 September 2018) available at <https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085>accessed 11 May 2019
Tim Berners-Lee, James Hendler and Ora Lassila, 'The Semantic Web' (Scientific American, May 2001) available at <https://www.scientificamerican.com/article/the-semantic-web>accessed 30 November 2018.
White House Office of Science and Technology Policy, 'Request for Information Regarding Data Portability: Public Responses' (White House Archives, 10 January 2017)
White House Office of the Press Secretary, 'Factsheet: President Obama's Precision Medicine Initiative' (White House Archive, 30 January 2015) available at <https://obamawhitehouse.archives.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative>accessed 17 December 2018.
William D. Eggers and others, 'Data as the New Currency' (Deloitte Insights, 24 July 2013) available at <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html>accessed 14 May 2019.
'What is Green Button' (Energy.gov) available at <https://www.energy.gov/data/green-button>accessed 17 December 2018.
Yasodara Cordova, 'Thoughts on personal data vs non-personal data' (The Medium, 1 April 2018) available at<https://medium.com/berkman-klein-center/thoughts-on-personal-data-vs-non-personal-data-9d84addfe820>accessed 10 May 2019
Zach Giesler, 'Loi N°2016-1321 Pour Une République Numérique: Regulatory Differences in French and EU Law' (Columbia Undergraduate Law Review, 19 November 2017) available at <http://blogs.cuit.columbia.edu/culr/2017/11/19/loi-n2016-1321-pour-une-republique-numerique-regulatory-differences-in-french-and-eu-law>accessed 19 February 2019.