Universiteit
Leiden
The Netherlands

Uncontrollable: Data subject rights and the data-driven economy

Ursic, H.

Citation

Ursic, H. (2019, February 7). *Uncontrollable: Data subject rights and the data-driven economy*. Retrieved from https://hdl.handle.net/1887/68574

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/68574

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/68574 holds various files of this Leiden University dissertation.

Author: Ursic, H.
Title: Uncontrollable: Data subject rights and the data-driven economy
Issue Date: 2019-02-07

Universiteit Leiden

Uncontrollable:

Data Subject Rights and the Data-driven Economy

Helena U. Vrabec

Uncontrollable:

Data Subject Rights and the Data-driven Economy

PROEFSCHRIFT

ter verkrijging van

de graad van Doctor aan de Universiteit Leiden,

op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,

volgens besluit van het College voor Promoties

te verdedigen op donderdag 7 februari 2019

klokke 10.00 uur

door

Helena Uršič

geboren te Šempeter pri Gorici (Slovenië)

in 1989

Promotor:	prof. dr. S. van der Hof
Co-promotor:	dr. ir. B.M.H. Custers
Promotiecommissie:	prof. dr. L. Edwards (Newcastle University, UK)
	prof. dr. E. Kosta (Tilburg Universiteit)
	dr. B.W. Schermer
	prof. dr. G.-J. Zwenne

Table of Contents

1. INTRODUCTION 15

1.1. The big data revolution and control over personal data 15

1.2. Research question(s) 18

1.3. Methodology 20

1.4. Introducing the main concepts 21

1.5. A cautionary remark regarding scope 22

1.6. Structure 23

2. THE RISE OF THE DATA-DRIVEN ECONOMY AND THE INDIVIDUAL 27

2.1. Introduction 27

2.2. Technologies that created the data-driven economy 28

2.2.1. Internet (of Things) 29

2.2.2. Datafication 30

2.2.3. Infinite data storage 31

2.2.4. Data analytics 32

2.3. How does the data-driven (big data) economy work? 33

2.3.1. Data acquisition 34

2.3.2. Data analytics and other software used to gain insights 36

2.3.3. Generating value through decision-making 38

2.4. The individual in the data-driven economy 39

2.4.1. Benefits 40

2.4.1.1. Convenience 40

2.4.1.2. Self-expression and self-control 41

2.4.1.3. Reduced cost and/or (in)direct monetary benefits 41

2.4.1.4. New knowledge and innovations 42

2.4.1.5. Security of data and citizens 43

2.4.2. Risks 43

2.4.2.1. Compromised privacy 44

2.4.2.2. Lack of transparency 45

2.4.2.3. Undermined autonomy 47

2.4.2.4. Power asymmetries 48

2.4.2.5. Discrimination 49

2.5. Conclusions 49

3. SAFEGUARDING INDIVIDUALS IN THE DATA-DRIVEN ECONOMY – LEGAL FRAMEWORK 53

3.1. Introduction 53

3.2. EU fundamental rights and personal data in the data-driven economy 54

3.2.1. Introduction 54

3.2.2. Protection of private life in the EU system of fundamental rights 57

3.2.2.1. The ECHR system of protection of personal data and private life 57

3.2.2.1.1. The right to private life under Article 8 of the ECHR 57

3.2.2.1.2. Protection of personal data under Article 8 of the ECHR 58

3.2.2.2. Privacy and data protection as part of the EU framework of fundamental rights 59

3.2.2.2.1. The right to private life and protection of privacy of personal data under Article 7 of the EU Charter 60

3.2.2.2.2. The right to data protection in Article 8 of the EU Charter 60
3.2.2.2.2.1. The reasons to codify data protection as a human right 61
3.2.2.2.2.2. Differences between the data protection right and the right to privacy 62
3.2.3. The prohibition of discrimination 65
3.2.4. Freedom of expression and thoughts 68
3.2.5. Consumer protection 69
3.2.6. Human dignity 70
3.2.7. The rule of law as the cornerstone of the EU human rights system – the relevance for the data-driven era 71
3.2.8. Freedom to do business 72
3.3. EU secondary law 73
3.3.1. Introduction 73
3.3.2. Data protection law 74
3.3.2.1. General data protection 74
3.3.2.1.1. Personal data at the heart of data protection law 75
3.3.2.1.2. Protection-oriented duties of commercial data users 77
3.3.2.1.2.1. Definitions of data users 77
3.3.2.1.2.2. Protection principles for personal data users 78
3.3.2.1.3. Control-enhancing rights of data subject rights 82
3.3.2.1.3.1. Definition of data subjects 82
3.3.2.1.3.2. Data subject rights 82
3.3.2.2. Protection of privacy in public communication networks (ePrivacy) 83
3.3.3. Cybersecurity provisions 84
3.3.4. Competition law 86
3.3.5. Consumer protection law 88
3.4. Conclusions 90
4. CONTROL AS A CENTRAL NOTION IN THE DISCUSSION ON DATA SUBJECT RIGHTS 93
4.1. Introduction 93
4.2. Roots of the term 94
4.2.1. Ordinary language and dictionary meaning 94
4.2.2. Control in philosophy 94
4.2.3. Control in psychology 95
4.3. Individual control over data and fundamental rights 97
4.3.1. Control over personal data and the right to informational self-determination 97
4.3.2. Control over personal data and the right to privacy 99
4.3.3. Control over personal data and the right to data protection 100
4.3.4. Control over personal data and the right to property 101
4.4. Control and EU data protection law 102
4.4.1. Policy vision for individual control in the data-driven economy 103
4.4.2. Reflections of control in the GDPR 104
4.4.3. Clustering control rights in the GDPR 105
4.5. Individual control – a challenging aspiration 107
4.6. Conclusions 107
5. THE RIGHT TO INFORMATION 111
5.1. Introduction 111

5.2. The link to fundamental values 112
5.3. Regulatory framework under the GDPR 113
5.3.1. The content of the communicated information 113
5.3.1.1. The information catalogue 113
5.3.1.1.1. Information about legal bases 115
5.3.1.1.2. Information about the length of the storage period 116
5.3.1.1.3. Information about third parties and recipients of data 117
5.3.1.1.4. Information about new (other) purposes of data processing 118
5.3.1.1.5. Information about the sources of data 120
5.3.1.2. The right to explanation 121
5.3.1.2.1. Information about automated decision-making in Articles 13 and 14 121
5.3.2. The quality of communication 124
5.3.3. The form of communicating the information provisions 127
5.3.3.1. Privacy policies and/or notices 127
5.3.3.1.1. Icons and other visualisations 129
5.3.3.1.2. Standardised privacy policies 131
5.3.3.1.3. Information incorporated in standard terms and conditions 132
5.3.4. Timing 133
5.3.4.1. When in time? 133
5.3.4.2. How often in time? 133
5.3.5. Restrictions 134
5.4. The right to information in the electronic communication sector 135
5.4.1. Privacy of electronic communication 135
5.4.2. Informing about placing the cookies and location tracking 136
5.4.3. Informing users about Wi-Fi tracking 138
5.4.4. Information on cybersecurity 138
5.5. The right to information as a control affording entitlement 139
5.5.1. Limits to data subjects' control 139
5.5.2. Enablers to data subjects' control 141
5.6. Conclusions 142
6. THE RIGHT OF ACCESS UNDER EU DATA PROTECTION LAW 146
6.1. Introduction 146
6.2. The right of access under the GDPR 148
6.2.1. The right of access under the GDPR 148
6.2.2. Examples of specific applications of right of access 150
6.2.2.1. The right of access on a continuum between personal and anonymised data 150
6.2.2.2. Accessing shared data and coupled databases 152
6.2.2.3. Access to information on automated decision-making 153
6.3. Regulatory boundaries of data subjects' data requests 155
6.3.1. Limitations regarding the cost, frequency, and scope of requests 155
6.3.2. Further exceptions 157
6.4. How the right of access works in practice 157
6.5. The right of access as a control affording entitlement 159
6.5.1. Limits to data subjects' control 159
6.5.2. Enablers to data subjects' control 160
6.6. Conclusions 161

7. THE RIGHT TO BE FORGOTTEN 165
7.1. Introduction 165
7.2. Values underpinning the RTBF 166
7.3. Towards the GDPR's version of the RTBF 167
7.3.1. The right to oblivion in criminal law 167
7.3.2. The RTBF under the data protection directive 168
7.4. The RTBF under the GDPR 168
7.4.1. The CJEU paving the way towards the GDPR in line with the 2012 proposal 168
7.4.1.1. Google Spain 169
7.4.1.2. Manni 173
7.4.2. The RTBF and its manifestations under the GDPR 174
7.4.2.1. Analysis of Article 17 of the GDPR – the right to erasure or the (explicit) RTBF 175
7.4.2.1.1. General 175
7.4.2.1.2. The meaning of 'informing third parties' 177
7.4.2.2. Other types of online 'forgetting' 180
7.4.2.2.1. The right to object 180
7.4.2.2.2. Consent withdrawal 181
7.5. Options to operationalise the RTBF beyond the GDPR 182
7.5.1. The right to a clean slate 182
7.5.2. Technical solutions to operationalise the RTBF 184
7.5.2.1. My Account by Google and Privacy Basics by Facebook 184
7.5.2.2. Deletion-by-default 185
7.5.2.3. Expiration dates 185
7.5.2.4. Obfuscation 186
7.5.2.5. Down-ranking 187
7.6. The RTBF as a control affording entitlement 187
7.6.1. Enablers to data subjects' control 187
7.6.2. Limits to data subjects' control 189
7.6.2.1. Technological forces 189
7.6.2.2. Economic forces 190
7.7. Conclusions 191

8. DATA PORTABILITY AS A DATA SUBJECT RIGHT 194
8.1. Introduction 194
8.2. How and when the idea of data portability emerged 195
8.2.1. Commercial initiatives 195
8.2.2. Regulatory initiatives 196
8.3. Personal data portability under the GDPR 197
8.3.1. Three components of the right 197
8.3.1.1. 'The […] right to receive the personal data […] in a structured, commonly used and machine-readable format' 197
8.3.1.2. '[…] the right to transmit those data to another controller without hindrance' 199
8.3.1.3. '[…] the right to have the personal data transmitted directly from one controller to another, where technically feasible.' 199
8.3.2. The restrictive definition of the right to data portability 200
8.3.2.1. '[…] data provided' 200
8.3.2.2. '[…] concerns a data subject' 201
8.3.2.3. 'The processing is based on consent […] or on a contract' 201

8.3.2.4. '[…]the processing is carried out by automated means' 202
8.3.2.5. 'The right should not apply to processing necessary for the performance of a task […] in the public interest or in the exercise of official authority […]' 202
8.3.2.6. 'That right shall not adversely affect the rights and freedoms of others.' 202
8.4. Data portability v. other data subject rights 203
8.4.1. The right of access 203
8.4.2. The right to erasure (the RTBF) 203
8.4.3. The right to information 204
8.5. Data portability in other legal fields 204
8.5.1. Data portability as a competition law measure 205
8.5.2. Data portability as another aspect of the right to access industrial data 207
8.5.3. Personal data portability at the intersection between consumer and data protection 209
8.6. The right to personal data portability as a control affording entitlement 210
8.6.1. Enablers to data subjects' control 210
8.6.1.1. Control over personal data transfers 210
8.6.1.2. Enabling control over (re)uses of data 211
8.6.1.3. Enabling control over multilevel data flows and complexity 213
8.6.1.4. Enabling free development of personality and equality 214
8.6.2. Limits to data subjects' control 215
8.7. Conclusions 215
9. DATA SUBJECT RIGHTS IN RELATION TO PROFILING 219
9.1. Introduction 219
9.2. Profiling as a building block of the data-driven value chain 219
9.2.1. The definition of profiling 219
9.2.2. Data science methods used for profiling 222
9.2.3. Risks of profiling 223
9.2.3.1. Possible harms 223
9.2.3.2. Profiling with no human intervention – the real danger? 224
9.3. How the GDPR tackles profiling on the individual level 225
9.3.1. The GDPR's definition of profiling 225
9.3.2. The difficulties with asserting the legal basis for profiling 226
9.3.3. Individual rights in relation to profiling 228
9.3.3.1. Hildebrandt's choice architecture 228
9.3.3.2. The right to object 229
9.3.3.3. The right not to be subject to solely automated decisions 232
9.3.3.3.1. The prohibition 232
9.3.3.3.2. The right to contest – technological due process? 235
9.4. Provisions on profiling as control affording entitlements 237
9.4.1. Enablers to data subjects' control 237
9.4.2. Limits to data subjects' control 237
9.5. Conclusions 238
10. CONCLUSIONS AND RECOMMENDATIONS 241
10.1. Introduction 241
10.2. (In)effectiveness of data subject rights 241

10.2.1. The effectiveness assessment 242
10.2.1.1. Data subject control rights as a vehicle of lawfulness, transparency and fairness, ... 243
10.2.1.1.1. Lawfulness 243
10.2.1.1.2. Transparency 244
10.2.1.1.3. Fairness 246
10.2.1.2. Data subject rights as a vehicle of purpose limitation 247
10.2.1.3. Data subject rights as a vehicle of data minimisation and storage limitation 248
10.2.1.4. Data subject rights as a vehicle of accuracy, integrity, and confidentiality 249
10.2.1.5. Data subject rights as a vehicle of accountability 250
10.2.2. Concluding remarks 250
10.3. The way forward for data subject rights 251
10.3.1. Abandoning control rights 251
10.3.2. Alternatives to data subject rights 252
10.3.2.1. Turning to technological solutions 252
10.3.2.2. Legal solutions 254
10.3.2.2.1. Holistic approach within the GDPR 254
10.3.2.2.2. Holistic approach outside the GDPR 255
10.3.2.2.2.1. Consumer protection 255
10.3.2.2.2.2. Competition law 257
10.3.2.2.2.3. Regulation of AI 258
10.3.3. Recommendations 258
Samenvatting (Dutch Summary) 260
Bibliography 263
Curriculum Vitae 288

Figure 1: Data-driven value chain 34
Figure 2: Privacy icons 130

Abbreviations

SME	Small and/or medium enterprise
EU	European union
DPD	Data protection directive
GDPR	General data protection regulation
ECHR	European Convention of Human Rights
CJEU	The Court of Justice of the EU
IoT	Internet of Things
AI	Artificial Intelligence
NHS	National Health Service
RFID	Radio-frequency ID
UK	United Kingdom
US	United States of America
NSA	US National Security Agency
ECtHR	The European Court of Human Rights
OECD	Organization for Economic Cooperation and Development
TFEU	Treaty on the functioning of the EU
NIS	Network and Information Security
EDPS	European Data Protection Supervisor
CMA	UK Competition and Markets Authority
DCD	Directive on Digital Content
LIBE	Committee on Civil Liberties, Justice and Home Affairs
RWD	Real-world data
DPA	Data protection authority
B2C	Business to consumer
ISO	International standardization organisation
NCC	National consumer council (Norway)
PbD	Privacy by design
RTBF	The right to be forgotten
URL	Uniform (Web) Resource Locator
ML	Machine learning

API	Application programming interface
EBF	European banking federation
DPaaS	Data portability as a service
FTC	Federal Trade Commission
ICT	Information and communication technology
CA	Cambridge Analytica
PIA	Privacy impact assessment
DPO	Data protection officer
EP	European Parliament
EC	European Commission
MP	Member of the Parliament

1. INTRODUCTION

1.1. The big data revolution and control over personal data

The tremendous growth in the amount of information and the means by which it can be disseminated has resulted in the transition from industry-based to information-based economies.[1] The transformation of data into a highly valuable asset[2] has created new business opportunities in the public and the private sector.[3]

In 2011, McKinsey released its breakthrough report, revealing that the data revolution had finally reached all economic sectors.[4] This announcement publicly recognised the continuing growth of the data economy, though the progress had been so obvious that it would have been difficult for anyone to miss it. The amount of data available in scientific fields such as biology and physics has increased far beyond anyone's imagination. For instance, the genetic sequencing data stored at the European Bioinformatics Institute has exploded.[5] In the past five years, it has risen exponentially up to 20 petabytes, doubling almost every year. Still, this represents just 10% of the tremendous amount of data stored at the CERN Swiss particle-physics laboratory.[6]

As noted by McKinsey, the data revolution has already had some profound consequences. It has affected how businesses value the data they hold and whom they allow to access it.[7] It has enabled, and even forced, companies to change their business models.[8] It has altered how organisations think about data and how they use it.[9] All of the largest Internet companies – Google, Facebook, Amazon, eBay, Microsoft, and Yahoo! – treat data as a major asset and source of value creation. In addition to tech giants, the big data revolution also offers room for the expansion of start-ups, small or medium enterprises (SMEs), and large, traditional corporations, especially those that deploy highly specialised analytic software able to scrutinise data in real-time.[10] Big data sharing, selling, and licensing have been seen as the great business opportunity of this era.[11]

Furthermore, the use of data can be beneficial for society as a whole. For example, using a robust database of 3.2 million individuals, researchers have managed to address the biologic factors linking parental antidepressant drug use to childhood autism spectrum disorders (ASDs).[12] Analysis of data showed that children who were exposed to their mother's use of antidepressants during the pregnancy had a much higher risk of developing ASDs.[13] The results of the study may affect the care of children

---

[1] Mark J Davison, *The Legal Protection of Databases* (Cambridge University Press 2008) 1.
[2] Ibid., 52.
[3] See for example OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) 11.
[4] McKinsey, 'Big Data: The next Frontier for Innovation, Competition, and Productivity' (2011).
[5] Vivien Marx, 'The Big Challenges of Big Data' (2013) 498 Nature 255.
[6] Ibid.
[7] Viktor Mayer-Schönberger and Keneth Cukier, *Big Data a Revolution That Will Transform How We Live, Work and Think* (Mariner Books 2014) 99.
[8] Ibid.
[9] Ibid.
[10] OECD, 'Exploring Data-Driven Innovation as a New Source of Growth' (2013).
[11] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 76.
[12] World Economic Forum, 'Unlocking the Value of Personal Data: From Collection to Usage' (2013) 8.
[13] Ibid.

and parents, given the total of over 4 million births per year in the US, and over 5 million births per year in European Union (EU) countries together.[14]

The clearest evidence of the data outburst can be seen in daily life. Instant messaging using mobile phones, easy access to documents through the cloud service, and personalised advertisements are all developments based on widespread data availability and reusability.

In the literature, these advances have often been described as the *big data revolution*.[15] The fundamental change is reflected in two recently coined terms: *data-driven* and *big data*. The terms convey two common trends. The first one is the existence of an *extraordinarily large amount* of available data. This data is too big (volume), arrives too rapidly (velocity), changes too fast (variability), contains too much noise (veracity), or is too diverse (variety) to be processed within a local computing structure using traditional approaches and techniques.[16] Later iterations of the definition have expanded to include new characteristics such as veracity and value. Particularly 'value' as a big data factor has grown in importance. Certainly, today's discussion on big data is mostly economically oriented. The burning question is how big data helps companies outperform competitors and how it creates value by unleashing the potential of hidden knowledge.[17] This leads to the second trend: *data analytics*. While traditionally, analytics has been used to find answers to predetermined questions (the search for the causes of certain behaviour, i.e., looking for the 'why'), analytics of big data leads to the finding of connections and relationships between data that are unexpected and that were previously unknown.[18] By employing sophisticated analytic techniques, data's value shifts from its primary use to its potential future uses or, as this thesis refers to them, *reuses*. Through the use of modern analytics tools, big data makes it possible to see patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions.[19,20]

Companies that base their business model on data reuse have exhibited particular interest in personal data. While this type of data is relatively easy to monetise, e.g. through behavioural advertising, it is also strictly regulated and protected on the human rights level.[21] This has been noticeably demonstrated in the EU, where it is believed that having control over personal data is a fundamental right.[22] However, the human rights dimension of data protection was not always dominant. When the EU was established as an economic union of the post-war Europe, its primary concern was a stronger economic integration, and first legal acts were drafted to unleash the potential of the common market.[23] As free movement of goods, capital, services, and people within the internal market required

---

[14] Ibid.

[15] Mayer-Schönberger and Cukier (2014). See also Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 240.

[16] Information technology ISO/IEC JTC 1, 'Big Data Preliminary Report 2014' (Geneva: ISO, 2015) 5.

[17] McKinsey, 'Big Data: The next Frontier for Innovation, Competition, and Productivity'.

[18] Lokke Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' 8 <https://www.debrauw.com/wp-content/uploads/NEWS - PUBLICATIONS/Moerel_oratie.pdf> accessed 14 June 2018.

[19] Kate Crawford and danah boyd, 'Six Provocations for Big Data', presented at Oxford Internet Institute's symposium *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* (Oxford 2011).

[20] While this thesis refers to big data in the sense of the '4-Vs definition' as explained above, in the literature big data is also described as an analytic phenomenon playing out in academia and industry. For the sake of clarity this thesis distinguishes big data and analytics by considering big data as raw material for analytics. Ibid.

[21] See Chapter 3, section 3.2.

[22] European Commission, 'How Does the Data Protection Reform Strengthen Citizens' Rights?' (2016) <ec.europa.eu/newsroom/just/document.cfm?doc_id=41525> accessed 25 May 2018.

[23] Luuk van Middelaar, *The Passage to Europe: How a Continent Became a Union* (Yale University Press 2013) 43.

free flow of data, it soon became urgent to reach a more detailed agreement on a uniform level of data protection.[24] Although the basic protection of data in Europe had already been set by the Council of Europe's Convention 108,[25] *Directive 95/46/EC 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* (DPD) adopted in 1995 importantly improved the legal environment by increasing the level of personal data protection and giving more substance to the Convention's vague principles.[26]

The adoption of the Lisbon Treaty[27] brought about significant changes to the legal regime governing personal data processing in the EU. Article 16 of the Treaty on the Functioning of the EU (TFEU)[28] introduced an explicit basis for the enactment of data protection legislation, while the Charter of the Fundamental Rights of the European Union (EU Charter)[29] set out the right to data protection in its Article 8, in addition to the right to privacy in Article 7.

In 2012, the European Commission published the proposal for the *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (GDPR).[30] The objective of the new law was to strengthen data protection and adapt it to the changed circumstances in the globalised and interconnected world. The vision that data protection is a fundamental right was one of the underpinning philosophies that drove the legislative process.[31] The regulation was adopted and published in the EU official journal in May 2016. It started to apply two years later, on 25 May, 2018.[32]

Like many other data protection legal instruments, the GDPR contains a section on the rights that the law grants to data subjects (i.e., persons whose data is (re)used). These rights – including the right to be informed, the right to erasure, the right to object, and the right to access – are significant legal developments, introduced in the 1970s when the first comprehensive data protection guidelines were adopted.[33] They are underpinned by an important vision, namely that individuals' control over their

---

[24] European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Data Protection Law* (2014) <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> 18.

[25] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (open for signature on 28 January 1981, entered into force on 1 October 1985).

[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 [1995] L C281/31.

[27] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007], OJ C 306/1.

[28] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/1.

[29] 2000/C 364/01 [2000] OJ C 364/3.

[30] 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) 1 final.

[31] Ibid., recital 1.

[32] 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) [2016] OJ L 119/1.

[33] A 1974 report by the Organisation for Economic Co-operation and Development (OECD) was one of the first prominent data protection documents that proposed a policy shift from the limited access approach to the control approach. See 'Policy issues in data protection and privacy: concepts and perspectives', proceedings of the OECD seminar 24th to 26th June 1974. At the same time in the US were developed the so-called 'fair information practice priciples,' a blend of substantive (e.g., data quality, use limitation) and procedural (e.g., consent, access) principles that set standards to facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society. Fred Cate, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of the Information Economy* (Routledge 2006) 343.

personal data is a constitutive part of the right to data protection. In fact, the idea of strong individual control over personal data has been highlighted as one of the key improvements of the GDPR. The European Commission's information factsheet stated: *'In this fast-changing environment, individuals must retain effective control over their personal data. This is a fundamental right for everyone in the EU and must be safeguarded.'*[34] However, in the light of the recent big data revolution, this idea faces a number of challenges.

The big data revolution and emergence of new business models have altered the rules of the game, not only for businesses but also for consumers, who have entered into a myriad of networks, applications, and databases.[35] In addition to willingly sharing their information online, consumers also leave many unintentional traces. In an online environment, more data is created about individuals than by individuals. In other words, the 'digital shadow' has outgrown the 'digital footprint'.[36] The intensity of personal data processing and its secondary uses have increased enormously. Data analytics can be used to 'help us' decide for whom to vote[37] or to track down Osama bin Laden.[38] New data-driven business models often go far beyond an individual user's understanding. Amidst this information outburst, consumers are inevitably losing control over their data.[39] The EU policy-makers[40] and some of the largest data processors[41] have been vocal about empowering data subjects, but the glossy language has not (yet) resulted in much change. However, the GDPR's strengthened and extended provisions on data subject control which started to apply in 2018 may lead to a shift.

This situation calls for a careful analysis of data subject rights under the new GDPR framework and their assessment through the lens of the current data-driven economic setting. Furthermore, it asks for a consideration of possible alternative approaches to data subject control that do not necessarily stem from data protection law. This thesis takes up this challenge.

1.2. Research question(s)

The main research question that this PhD study seeks to answer is the following:

---

[34] European Commission, 'How Does the Data Protection Reform Strengthen Citizens' Rights?' (2016).
[35] It has been observed that the current regulation may not sufficiently address the challenges related to big data sets. See for example Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74; Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2018) 94 Seton Hall Law Review 995.
[36] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice' (2011) 8 SCRIPTed.
[37] Will Oremus, 'The Real Scandal Isn't What Cambridge Analytica Did' *Slate.com* (March 20, 2018) <https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html> accessed 22 May 2018.
[38] Jacob Choi, 'Palantir – Big Data Possibly Helped Catch Bin Laden' (*Stanford MS&E 238 Blog*, 28 July 2017) <https://mse238blog.stanford.edu/2017/07/jchoi8/palantir-big-data-possibly-helped-catch-bin-laden/> accessed 23 May 2018.
[39] Mobile Ecosystem Forum, 'MEF's Global Consumer Trust Survey 2016/7' (2017) 8 <https://mobileecosystemforum.com/wp-content/uploads/2017/06/MEF_Global_Consumer_Trust_Report_2017.pdf> accessed 27 December 2018; also see Kaspersky Lab, 'The State of Cyber-Stress' (2018) <https://media.kaspersky.com/en/state-of-cyber-stress-survey-report.pdf> accessed 27 December 2018.
[40] European Comission, 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Business' <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en> accessed 23 May 2018.
[41] Julie, Bril (JulieSBril) 'Microsoft to apply #GDPR worldwide' *Twitter* (22 May 2018) <https://twitter.com/JulieSBrill/status/998966587385262080> accessed 26 May 2018.

Are the data subject rights under the EU law effective in the data-driven economy?

This key question is broken down into a set of sub-questions to provide a more detailed explanation of the research objectives and to sketch the research outline. The first sub-question focuses on the notion of the data-driven economy, one of the key terms used throughout this study:

(1) What is the data-driven economy and how does it work and evolve?

This sub-question refers, first, to the driving forces behind the rise of the data economy, and second, to the position of the data economy, taking into consideration its technological enablers, economic rationales, societal consequences, and the interdependencies among them. Although the focus is on the experiences on the EU level, the influence of some foreign economies cannot be disregarded.

The second sub-question shifts attention to the positive law:

(2) What is the relevant EU regulatory framework for the data-driven economy from the perspective of an individual, with particular regard to the protection of individuals and their personal data?

This sub-question builds on the assumption that not only data protection law but also legal provisions outside the scope of privacy laws are relevant for the protection of individuals in the data-driven economies. The objective is to obtain a solid understanding of the rules that underpin the relations and transfers of information goods in the data economy. These relevant legal provisions may work in two ways: first, as a restraint for the businesses on the data-oriented market, and second, as a means of protection for individuals and their personal data.

The focus of this thesis is on the control rights that the EU data protection law grants to individuals in the data-driven online environment. Therefore, the research sub-questions are structured in a way that gradually leads from a general, theoretical exploration of control to a more detailed analysis of these specific rights. The general exploration of control is part of the third sub-question:

(3) What does the notion of individual control entail and, specifically, how does it relate to the discussion on data subject rights?

The purpose of this sub-question is to create a bridge between the general illustration of the economic reality on the data-driven market and the specific legal provisions on data subject control rights. This is done by elaborating on the concept of control and taking into consideration philosophical, psychological, and legal thought. In particular, this sub-question explores the relation between the notion of control and data subject rights. The answer serves as an introduction to the fourth sub-question:

(4) What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?

The question specifically refers to the rights under the GDPR and takes into consideration broader technological and economic implications. In particular, this question seeks to explore the extent to which these rights are successful in facilitating data subject control in the data-driven economy. By doing so, it sets the basis for the fifth and last research sub-question:

(5) Are data subject rights granted by EU law effective and if not, what are possible solutions?

Drawing on the insights from the previous answers, the final sub-question triggers an assessment of the effectiveness of data subject rights under EU law. Depending on the findings, some viable solutions are offered, stemming from data protection law as well as some other legal areas.

1.3. Methodology

Two key methods used in this thesis are (1) desk research of (academic) literature and (2) analysis of relevant legal sources and case law.

The first method, desk research, refers to the review of academic journal papers, books and journalistic texts gathered from multiple scientific databases and repositories, both public and private.

Amongst the private sources, the key one was the digital repository of the Leiden University library[42], consisting of roughly 23.000 physical items and 25.000 electronic journals.[43] This large database was analysed by using key search terms including but not limited to 'data economy', 'data subject', 'the right to be forgotten', 'the right to objection', 'automated decision-making', and 'individual control'. In addition, Yale Law School digital database[44] was used in the final stage of the study with the focus on US authors. The Yale Law School data was analysed using the same search terms as for the analysis of the Leiden repository.

Amongst the public sources, the focus was on the following three research databases: Google Scholar,[45] WorldCat,[46] and Social Science Research Network[47]. To analyse these public databases, the same key search terms were used as above. That said, the success rate for identification of the relevant literature was lower. Although the search results provided a larger number of listed sources, the content of many was not freely accessible.

Regardless of whether a public or a private database was used, the focus was on the recent scholarship. 'Recent' stands for sources with the publishing date no earlier than 1 January 2000. However, in some situations less recent papers were considered as well. In particular, a less recent source was used when it was recognized as fundamental literature based on a high citation rate. An example is Adam Westin's 1969 book Privacy and Freedom. According to Google Scholar, it has been cited 12.800 times since 1998. The final date until which the literature was considered was 1 August 2018.

When the study dealt with recent issues that have not yet been addressed in a published academic journal paper or book, a limited number of non-scientific and journalistic texts was used as

[42] https://www.bibliotheek.universiteitleiden.nl/.
[43] https://www.bibliotheek.universiteitleiden.nl/over-ons/feiten-en-cijfers.
[44] https://library.law.yale.edu/.
[45] https://scholar.google.de/.
[46] https://www.WorldCat.org.
[47] https://ssrn.com/en/.

complimentary literature. The sources were identified by conducting an analysis of the world leading newspapers,[48] news portals[49] and web blogs[50].

The goal of desk research as a research method was to acquire the necessary theoretical knowledge. As a consequence, this method is prevalent in the first chapters of the thesis, particularly in Chapters 2, 3 and 4.

The second research method was the analysis of relevant legal sources and case law conducted with the help of the official EU law database[51] and the published case law available via the European Court of Justice database.[52] The scope was thus limited to EU legal sources. That said, the legal research occasionally departed from the chosen standpoint and drew attention to national specifics that might have had an impact on EU policy. This was unavoidable due to strong co-dependency between the EU regulation and member states' national laws. In those infrequent cases, relevant national legislation and case law were also considered. Such national provisions were mostly identified in or referred to by academic papers. The analysis of legal sources was mostly used to answer the research questions in Chapters 3, 5, 6, 7, 8, and 9. The final date until which the legal sources and case law were considered was 1 August 2018.

Besides the two main methods mentioned above, this study also applied, to a limited extent, comparative legal research between EU and US law. The US legal system serves as an example of a legal regime which has a similarly wide reach but substantially differs from the EU approach to data protection. Most obviously, the US law is based on the common law system which to a larger extent depends on the rule of precedent and judge-made law. Especially in privacy law, some important US legal doctrines were shaped entirely through case law. Comparative legal research, as a complimentary research method, appeared in parts of chapters 3, 4, 5, 8, and 9.

1.4. Introducing the main concepts

At the outset, the key terms contained in the key research question need to be clarified. These terms are data-driven economy, data subject, and data subject rights.

Data-driven economy serves as an umbrella term for businesses that perform data (re)use as their core activity. Since data-driven economy as a term only appeared recently, its definition has not been fully established yet. Nonetheless, it is important to bear in mind that the focus of the data-driven economy is always on the secondary use of data, i.e. business models that seek to utilise the existing data in innovative and profitable ways. Business activities where data is only generated, collected, or stored are therefore not of interest.

The terms data-driven economy, big data economy and data economy are used interchangeably in this thesis. However, data-driven is not always a synonym for big data. Data-driven refers to business models that use data as a resource, regardless of what type of data it is (structured or unstructured,

[48] E.g., The Economist, The Guardian, The New York Times, The Financial Times.
[49] E.g., BBC.com, CNN.com, Volkskrant.nl.
[50] E.g., Hunton Privacy Blog (https://www.huntonprivacyblog.com/), Fieldfisher Privacy Blog (http://privacylawblog.fieldfisher.com/), IAPP Privacy Perspectives (https://iapp.org/news/privacy-perspectives), Leiden Law blog (http://leidenlawblog.nl).
[51] http://eur-lex.europa.eu/homepage.html.
[52] http://curia.europa.eu/jcms/jcms/j_6/.

handled manually or processed by computer, personal or industry data, etc.). Big data refers specifically to vast amounts of data which are particularly useful as a source for analytics and data-driven decision-making. Big data is thus only one part of all possible types and uses of data. However, in today's economic reality, big data sets are those that are most likely to accrue value and where secondary results occur most easily, e.g. as marketing predictions or sales of data.[53] Big data is what data-driven companies are most interested in. For this reason, data-driven most often equals big data.

Chapter 2 explores the definition and broader impacts of the data-driven economy in more detail.

Data subjects are identified or identifiable natural persons who can in particular be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity.[54] This study uses the term 'data subjects' interchangeably with the terms 'individuals' and 'consumers', as in the majority of the situations they overlap. When the difference is decisive, however, this is indicated.

Chapter 3 explains each component of the definition of a data subject as provided in EU law.

Data subject rights normally refer to the group of rights that data protection law grants to individuals such as the right to access and the right to object. These rights have formed the core of the data protection law since its very beginnings and have found their way into a large number of data protection statutes all over the world.[55] Chapters 3 to 9 of this thesis describe their historical development, ethical, and in particular economic justifications, along with the current legal framework.

1.5. A cautionary remark regarding scope

This thesis is only concerned with the implications of the data-driven economy for *data subject rights* and does not address other relevant dilemmas of data protection law or any other law related to the data economy.

The scope of the legal analysis is limited to EU law. It does not extend to legislations on any other continent, nor does it consider national specifics in the EU member states, although at times it does reflect on some of them to better illustrate a European provision. The European Convention on Human Rights (ECHR)[56] and related jurisprudence is understood as an integral part of EU law.

EU law was chosen as the basis of this study for two major reasons. First, although the EU is a union of sovereign states with their own national laws, the rules on the EU level are common to all member states and act as a reflection of the EU consensus on adequate legal standards. This approach has been confirmed by the doctrine of direct effect of the EU legislation.[57] Through this doctrine, the Court of Justice of the EU (CJEU) has established that the EU regulations are directly applicable and should be interpreted coherently throughout the Union.[58] Second, while it is clear that the European market is

[53] Mayer-Schönberger and Cukier (2014).
[54] Article 4 (1) of the GDPR.
[55] Compare Borgesius (2014) 88, 133.
[56] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).
[57] Damian Chalmers, Gareth Davies and Giorgio Monti, *European Union Law: Cases and Materials* (Cambridge University Press 2010) 285.
[58] C-6/64, *Flaminio Costa v E.N.E.L.* [1964] ECLI:EU:C:1964:66.

legally, economically, and culturally fragmented, the general perception and political tendency is to see it as a single market. In recent years, the idea of a single digital market has been placed high on the EU political agenda.[59] It is believed that more harmonised legal provisions in the digital realm would grant more protection to citizens and reduce the administration cost for European businesses. The recently approved data protection regulation, which advocates unified standards and more collaboration between member states, supports this idea.

This thesis focuses on data (re)use in the private, commercial sector. It does not deal with data (re)use for the purpose of law enforcement or of any other public service. It does, however, acknowledge the significance of public data for commercial organisations and possible legal challenges that may occur as a consequence of sharing public data with private parties. This relation is addressed in more detail in section 3.1.

Not all control rights listed in the GDPR are subject to analysis in this thesis: only six are analysed and commented upon in detail. Specifically, the right to rectification in Article 16 of the GDPR and the right to restriction of processing in Article 18 of the GDPR are excluded from the scope. This is not to say that these rights are irrelevant in the light of the big data discussion. The reason for the exclusion is that they share similarities with the right to erasure (Article 17) and the right to object (Article 21). Thus, their limitations and prospects are, to a large extent, reflected in the analysis of the rights in Articles 17 and 21.

Finally, this thesis does not (systematically) investigate legal enforcement of the rights, apart from those cases that have already been adjudicated by the CJEU. This is because a thorough analysis of legal enforcement across all member states would require a considerably broader and longer study. Another reason is that the GDPR only recently started to apply. As the case law is still evolving and regulatory decisions are scarce, legal analysis is challenging and incomplete. However, the issue of law enforcement could be the subject of important follow-up research. After all, the GDPR is not only a new law, but a shift in the global perception of privacy. In the years to come, this study's findings will probably need to be revised in light of the GDPR's future enforcement.

1.6. Structure

Chapter 1 introduces the topic of this thesis, elaborates on the research questions, explains the key concepts, presents the methodology, and outlines the structure.

Chapter 2 answers the first research sub-question by addressing the notion of data-driven economy from three different perspectives. First, the technological dimension of this economy and its key components are explored. Second, the economic dimension is explained through the analysis of the data-driven value chain. Using some practical examples, the chain is analysed starting at the data acquisition stage and ending at the data-driven value generation stage. Finally, the advantages and threats that data-driven business models impose on individuals are examined in more detail.

Chapter 3, which focuses on the second research sub-question, thoroughly and concisely assesses the EU legal framework for the data economy. The aim of the assessment is to identify provisions that have

[59] European Commission, 'Digital single market: Bringing down barriers to unlock online opportunities' <https://ec.europa.eu/commission/priorities/digital-single-market_en> accessed 26 May 2018.

an impact on individual control over personal data processing. The first part of the chapter deals with primary sources such as human rights provisions; the second part turns to secondary legislation, paying special attention to EU data protection law. As mentioned above, non-EU legal sources and national legislation are in principle excluded from the scope of the legal framework.

Chapter 4 deals with the third research sub-question and discusses the concept of individual control including its legal and ethical justifications. Most importantly, the chapter provides an explanation why data protection law can be seen as one of the most evident expressions of control over personal data. Furthermore, the chapter structures the GDPR's control-related provisions and sets the stage for their further analysis.

Chapters 5-9 focus on the fourth research sub-question and thoroughly explore the entitlements which data subjects enjoy under the EU data protection laws and the implications that the data-driven economy has for them. In addition, the chapters discuss whether the rights succeed or fail at facilitating data subject control. The focus is on six rights provided in the GDPR: the right to information, the right to access, the right to data portability, the right to erasure, the right to object, and the right not to be subject to automated decision-making.

Finally, Chapter 10 answers the fifth research sub-question regarding the effectiveness of data subject rights in the data driven economy and indicates possible alternatives. To determine whether the legal provisions on data subject rights offer any meaningful protection to data subjects, the chapter first introduces a framework to assess the effectiveness of the rights. While effectiveness is a broad term that can have many meanings, this thesis is concerned with the effectiveness in terms of data subjects' *control* over their data. When ineffectiveness is spotted, a number of solutions and innovative measures are proposed to strengthen data subject control in the future. In this regard, the chapter explores some technical tools, controllers' protection duties imposed by the GDPR, and solutions outside the limited scope of data protection law. By summarizing the findings from previous chapters with regards to the implications of the data-driven economy for the data subject rights and connecting these findings with the effectiveness analysis, Chapter 10 also provides a complete answer to the key research question.

2. THE RISE OF THE DATA-DRIVEN ECONOMY AND THE INDIVIDUAL

2.1. Introduction

Some see the 21st century as a new industrial and economic era.[60] In their view, the recent technological developments – social media, connected devices, datafication, and ubiquitous computing – have been so significant that they have opened the way for the next technological revolution and set the basis of an entirely new industry.[61] As Klaus Schwab, the founder of the World Economic Forum, puts it, *'a fusion of technologies that is blurring the lines between the physical, digital and biological spheres has characterized a fourth industrial revolution …'* .[62]

The change between the world in the 1990s and the world of today is undoubtedly apparent. Consider a simple example: a TV device. In the 1990s, almost every household owned a large, clumsy, and heavy device which emitted a high level of electromagnetic radiation and offered, by today's standards, the bare minimum of picture quality. Today, users have witnessed a new generation of televisions: devices with flat screens. Moreover, a TV is no longer solely a TV. Shows, movies, video games, apps, streaming, and more – all of this is available to a TV user simply by swiping on a touch screen. TVs have become smart devices that understand users' wishes and communicate with other devices. However, TVs are also smart for another reason: they are able to work behind the scenes. Ceaselessly and quietly, TVs collaborate with their manufacturers and share data about users' watching habits. The same data can later be sold to a third party, e.g. an advertiser. Vizio, a California-based TV maker, was recently found to follow such commercial tactics.[63] The company tracked customers in a way that enabled it to connect their viewing habits to their IP addresses.[64] Advertisers that were given access to this data were able to target users through several different mobile devices.[65]

Regardless of whether data-driven strategies are seen as a new stage in the history of the world's industry or as a continuation of the digital revolution, one thing is certain: the role of data in the economy is becoming much more pervasive. As demonstrated by the example above, the possibility of

---

[60] See for example Dirk Helbing, 'Economy 4.0 and Digital Society: The Participatory Market Society Is Born (Chapter 8 of Digital Society)' [2014] <http://papers.ssrn.com.ezproxy.liv.ac.uk/sol3/papers.cfm?abstract_id=2539330> accessed 27 May 2018.

[61] Klaus Schwab, 'The Fourth Industrial Revolution: what it means, how to respond' World Economic Forum (14 January 2016) <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> accessed on 27 May 2018.

[62] Ibid.

[63] Ellie Zolfagharifard, 'Is YOUR TV spying on you? Report reveals how Vizio smart televisions track your data so that it can be sold to advertisers', *DailyMail* (10 November 2015) <http://www.dailymail.co.uk/sciencetech/article-3312597/Is-TV-spying-Report-reveals-Vizio-smart-televisions-track-data-sold-advertisers.html#ixzz4Ij0DiJQe> accessed on October 15, 2016.

[64] '*An Internet Protocol address ("IP addres") is a sequence of binary numbers which, when allocated to a device (a computer, a tablet or a smartphone), identifies it and allows it to access that electronic communications network. The device, in order to connect to the Internet, must use the number sequence provided by Internet service providers. The IP address is transmitted to the server on which the accessed web page is stored*.' C-582/14 *Patrick Breyer v Bundes republik Deutschland* [2016] ECLI:EU:C:2016:339, Opinion of AG Campos Sánchez-Bordona, para. 1.

[65] In 2013 LG advertised its smart TV by praising its ability to target advertising based on the profiles built on the data that is collected during the use of the TV: '*LG Smart Ad can feature sharp suits to men, or alluring cosmetics and fragrances to women.'* 'LG Smart TVs logging USB filenames and viewing info to LG servers' (*Blogspotcom*, 18 November 2013) <http://doctorbeet.blogspot.com/2013/11/lg-smart-tvs-logging-usb-filenames-and.html> accessed 27 May 2018.

secondary uses gives big data a new function and opens up business opportunities that were previously unimaginable.

Despite its great potential, big data use is not always innocent and beneficial to individuals. From the latter's perspective, its use can also be risky, ethically disputable, and sometimes illegal. The following sections of this chapter provide examples of all three situations.

By exploring the drivers of big data and the position of individuals in the data-driven economy, Chapter 2 answers the first sub-question of this thesis: *What are the driving forces behind the rise of the data-driven economy, taking into consideration technological enablers, economic consequences, and their interdependencies, and what are the consequences for individuals?* For the sake of clarity, the answer is split into three sections.

Section 2.2. focuses on three technological enablers that have led to the data revolution: the Internet, datafication, improved storage capabilities, and analytics. The aim here is not to go into technical details but to provide some background information that will be useful in the further analysis of legal responses to technological developments. As the intention is to illustrate the role individuals play in the data economy, technical developments are only explained to the degree that allows a meaningful demonstration of possible impacts on individuals. Indeed, even more than written norms imposed by a regulator, technology can strengthen or weaken an individual's position, which is a plausible reason for a brief analysis.[66]

After the technology-focused section, section 2.3. explains how the data-driven economy works. To simplify the complex economic ecosystem, an illustration of a data value chain consisting of three links is used: 1) data generation and acquisition, 2) analysis of data, and 3) data-driven decision-making. The key point is to understand why, from a business perspective, (personal) data can be a useful source of information and how the use of (personal) data has influenced the economy.

In the final section (2.4.), the focus is on individuals as an important group of actors in the data economy. It is shown how the data economy can work to both their advantage and disadvantage. Knowing more about risks and benefits is critical before taking on a legal discussion, which shifts the focus to addressing and mitigating the risks.

2.2. Technologies that created the data-driven economy

The sections below reflect upon four technological pillars that form the foundation of the data economy: the Internet, indefinite data storage, datafication, and data analytics. Undoubtedly, many more technologies have contributed to the rapid change in the data economy, such as advanced software and networks infrastructure. However, as the scope of this chapter is limited, these are not explained in more detail.

[66] Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006). For example, in a recent interview Lessig praises Enigma, a decentralized cloud platform based on blockchain technology, for its privacy-enhancing invention. Their system could address problems which laws cannot. Steve Rosenbush, 'Lawrence Lessig: Technology Will Create New Models for Privacy Regulation' *The Wall Street Journal* (30 December 2015), <https://www.wsj.com/news/cio-journal> accessed 27 May 2018.

2.2.1. Internet (of Things)

The Internet or, more specifically, the World Wide Web is one of the fundaments of the data economy.[67] Its foundations were laid by Tim Berners-Lee's invention of the hypertext markup language in 1989, which created an open system platform where data and information could be shared and accessed instantaneously across the world.[68] This opened up new possibilities for the economy.[69] Today, the power of the Internet is amplified due to the rapid diffusion of broadband creating the underlying infrastructure for the exchange and free flow of data.[70] Data collected remotely through Internet applications and now increasingly through smart and interconnected devices can be easily shared and transferred all around the world.[71]

Not only the industry has benefited from the Internet: users who were once passive have also been given exciting opportunities to take a more active role on the Internet.[72] By using modern and greatly improved technologies, they have become more directly involved in content generation and sharing.[73] This user-friendly and social networking web, also known as Web 2.0,[74] has led to an increased opportunity to capture personal data. The more active the users are, the richer the data they leave behind.

The Internet is still evolving. The latest era in the Internet history is the so-called Internet of Things (IoT) or ubiquitous computing.[75] IoT stands for 'things' such as devices or sensors that connect, communicate, or transmit information with or between each other through the Internet.[76] IoT is fuelled by the prevalence of devices enabled by open wireless technology such as Bluetooth, radio-frequency identification,[77] Wi-Fi,[78] and telephonic data services, along with embedded sensors.[79] These machines

---

[67] Many people use the words 'Internet' and 'the World Wide Web' interchangeably. While they are indeed linked, they are two separate phenomena. The Internet is a global system of interconnected computer networks using the Internet protocol suite (TCP/IP) to link devices. The World Wide Web ('www' or 'web' for short) is a set of protocols and conventions which creates a universe of network-accessible information. The web is easy for anyone to roam, browse, and contribute to through the use hypertext and multimedia techniques, and can be accessed via the Internet by using web browsers such as Google Chrome, Internet Explorer or Mozilla Firefox. Lessig (2006) 145-146. Also see 'About World Wide Web' W3C, 24 January 2001 <https://www.w3.org/WWW/> accessed 14 June 2018.

[68] Lessig (2006) 146.

[69] Leo Bartevyan, 'Industry 4.0 – Summary Report' (2015) <https://www.cenit.com/fileadmin/dam/Corporate/PDFs/2015_5_Expertenwissen_E.pdf> accessed 27 May 2018.

[70] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 35. Broadband is a high-speed communications network and especially one in which a frequency range is divided into multiple independent channels for simultaneous transmission of signals (as voice, data, or video). Definition from Merriam-Webster online dictionary <https://www.merriam-webster.com/dictionary/broadband> accessed on December 28, 2016.

[71] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 35.

[72] Angela Daly, 'The Internet, User Autonomy and EU Law' (2016) <https://www.ssrn.com/abstract=2780789> accessed 27 May 2018.

[73] Bartevyan (2015).

[74] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009).

[75] Sometimes also called the Internet 3.0 or 4.0., see for example J Gubbi and others, 'Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions' (2013) 29 Future Generation Computer Systems 1645.

[76] FTC, 'Internet of Things: Privacy & Security in a Connected World' (2015) 5.

[77] A tag containing a unique ID. If it is destined to be carried by a person, then the tag ID should be considered as personal data. Article 29 Data Protection Working Party, '*Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*' (2011).

[78] In particular the wireless sensor network, which stands for a network of nodes that cooperatively sense and control the environment, enabling interactions between persons or computers and the surrounding environment.

[79] Gubbi and others (2013).

have the potential to produce more and more data and to create new opportunities for their employment and application. Personal data represents a huge amount of the data captured in the IoT.

IoT indicates an interesting shift in the history of the Internet. While Web 1.0 was not yet developed to the degree that would enable *individuals* to be active users, Web 2.0 changed this as it gave individuals tools to be more engaged online. In the era of IoT or Web 3.0, the trend has reversed. Individuals are becoming less involved because data processing typically takes place behind the scenes, e.g. by generating information through multiple omnipresent sensors. In recent years, the IoT has become so sophisticated that a random user hardly notices it. In fact, it is the point of IoT to be hidden from a user's view. What is also revolutionary is that these physical information systems are now starting to be deployed, and some of them even work largely without human intervention.[80] Nevertheless, individuals can still be deeply involved in and dependent on these processes.[81] As mentioned above, data collected in the IoT environment very often relates, directly or indirectly, to individuals. For instance, after discussing babies in front of Amazon's personal assistant Alexa, a husband started receiving advertisements for Seventh Generation diapers on his Amazon Kindle.[82] Clearly, the devices were somehow connected, most likely via his email address. Having analysed the exchanged data, the device was able to predict the couple's highly personal plans and wishes.

2.2.2. Datafication

Over the past decade, digital data production and storage have grown exponentially.[83] However, another process has run in parallel to data increase: digitalised data has been translated into discrete, machine-readable, measurable, manipulable bits and bytes.[84] Putting data into a quantified format has enabled its tabulation and analysis. This transformation is commonly referred to as *datafication*.[85] The process of datafication started in the financial, energy, and retail industries,[86] but it soon expanded to other areas. In recent years, we have witnessed the datafication of words, markets, locations, and even human interactions.[87]

Individuals engage in the process of datafication by contributing their personal data as raw material. Every online appearance leaves a digital trace, which gradually grows into a vast registry of the actions constituting 'data doubles' or 'quantified selves'.[88] The process of *personal datafication* – a

---

[80] McKinsey, 'Big Data: The next Frontier for Innovation, Competition, and Productivity'.
[81] Rebecca Crootof, 'An Internet of Torts' (2018) <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Crootof-An-Internet-of-Torts-We-Robot-Submission.pdf>.
[82] Rory Carroll, 'Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all' *The Guardian* (21 November 2015) <https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud accessed> 27 May 2018.
[83] Peter Géczy, 'Data Economy Dimensions' (2015) 9 Global Journal of Business Research.
[84] Mireille Hildebrandt, 'Slaves to Big Data. Or Are We?' [2013] IDP Revista De Internet, Derecho I Política 6.
[85] To illustrate the distinction between digitalisation and datafication we can use the example of a book copy. When the original book is scanned to make a digital copy, this is called digitization. Datafication of a book goes a step further by making the text indexable and thus searchable. Mayer-Schönberger and Cukier (2014) 144.
[86] Jeff Bertolucci, 'Big Data's New Buzzword' *InformationWeek* (25 February 2013) <http://www.informationweek.com/big-data/big-data-analytics/big-datas-new-buzzword-datafication/d/d-id/1108797> accessed on 25 May 2018.
[87] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75, 79.
[88] Gemma Galdon Clavell, 'Policing, Big Data and the Commodification of Security' in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 106. Also see Sara M. Watson, 'How Close Does Personalized Online Advertising Get to us as Our Real Persons?' *Schirnmag* (21 May 2016) <http://www.schirn.de/en/magazine/context/sara_m_watson_bits_of_me_essay/> accessed on October 3, 2016. Watson

transformation into data of multiple aspects of the lives of individuals[89] – has been the focus of a growing number of consumer-centred companies. Large Internet-based firms such as Google and Facebook are the most obvious example of the trend, but smaller Internet start-ups do not lag far behind.[90]

Datafication of personal information and behaviour is inherent to the process of personal data commodification and commercialisation. Commodification means exchanging data for something else, thus transforming datafied information into (monetary) value. Taking the form of a commodity, personal data is devaluated to the level of a commercial good. As the next chapter explains in detail, personal data is a concept granted human right protection.[91] Hence, its commodification and commercialisation can be seen as problematic *per se.*[92]

2.2.3. Infinite data storage

The 'datafication' of society and the advance of big data go hand in hand with the decreased costs of data management and data storage hardware and software. Exponential increases in computer capabilities, also referred to as Moore's law, created opportunities to build massive databases.[93] Today, data rendered in digital form can be stored for indefinitely long periods of time and can be readily retrieved.[94] To map and process large data sets, companies have developed powerful software such as Apache Hadoop integrating a MapReduce programming model.[95]

Databases are not necessarily stored locally but can be easily moved onto the Internet. Cloud computing describes a storing, processing, and use of data on remotely located computers accessed over the Internet.[96] Outsourcing data storage to an Internet service provider reduces cost and allows companies to collect data on a much larger scale.

The continuously changing Internet and rapid transformations of digital technologies create a perception of ephemerality of everything that happens online. The reality, however, is the opposite. Data shadows left behind individuals are increasingly difficult for those very individuals to shape, delete, or fully control. This is, in the first place, a consequence of the possibility of indefinite storage of personal information. However, the situation is escalated because data is typically moved and stored

---

writes about her doppelgänger – a digital representation of herself that commercial parties as well as the Government can reconstruct from the tracks she leaves on the internet: *'She is between the ages of 25–34. Or she's under 32. She is a millennial. She's inferred married. But she uses her phone like a single lady. She has eight lines of credit and is an upscale card holder. She's into coupons. She has recently purchased party goods, personal care products for men, and women's plus-sized apparel. She only walked 40,094 steps last week. She might qualify for a medical study on anorexia*.'

[89] Directorate General for Internal Policies, 'Big Data and Smart Devices and Their Impact on Privacy' (European Parliament 2015) 11.

[90] Zuboff, 77.

[91] See more in Chapter 3, section 3.2.

[92] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' <https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf> accessed 13 November 2017. In addition, problems may arise as a result of commodified data's secondary uses – see more in section 2.4.2. of this chapter that discusses some relevant risks.

[93] OECD, 'Exploring Data-Driven Innovation as a New Source of Growth' 10.

[94] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 36.

[95] Kanala Urmila and Sandhya Rani, 'Hadoop Technology for BigData Analytics' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3168340> accessed 27 December 2018.

[96] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe' (2012).

in a cloud, where it is kept away from the physical reach of a user. Although cloud storage often proves convenient, e.g. when a user migrates her data from an old to a new device, it decreases the transparency of data processing and increases the safety risk as data is transferred over the Internet.[97]

2.2.4. Data analytics

As mentioned in the previous chapter, analytics is inherent to big data (data-driven) business models.[98] ENISA's definition of big data emphasises this, describing big data as *'the technologies, the set of tools, the data and the analytics used in processing large amount of data.'*[99] Data analytics is an umbrella term for various methods of information and knowledge extraction from large volumes of data to improve decision-making. Data mining is one of the analytical techniques used to analyse big data.[100] The goal of data mining is to discover previously unseen patterns and relationships from large datasets and to derive business value from these.[101] If these patterns or correlations are used to identify or represent people, they are referred to as *profiles.*[102] Analytical software offers several methods to perform data mining: statistical methods, e.g. regression and clustering, but also more sophisticated methods such as machine learning.[103] In machine learning, the machine automatically learns the parameters of models from the data using self-learning algorithms to improve its performance at a task with experience over time.[104] The discussion on data analytics is not complete without mentioning artificial intelligence (AI). AI incorporates machine learning and other disciplines such as robotics and natural language understanding; it is a broader concept of machines being able to carry out tasks in a way that would be considered 'smart'.[105] Today, AI is used in many contexts but most often to describe new, sophisticated technologies such as home assistants and autonomous weapons.

What makes all these big data techniques particularly valuable is the possibility of prediction.[106] Google's search engine, which uses anticipatory algorithms to predict what information users want based on a combination of data like website popularity, location, and prior search, is a prime example

---

[97] Christl writes about the use of Oracle's cloud, where data service providers upload their own data about customers, website visitors, or app users, combine it with data from many other companies and then transfer and utilize it on hundreds of other marketing and advertising technology platforms in real-time. This data can be used to, for example, find and target people across devices and platforms, personalize interactions, and eventually, to measure how consumers respond after having been addressed and affected on an individual level. Wolfie Christl, 'Corporate Surveillance in Everyday Life' *CrackedLabs* (June 2017) <http://crackedlabs.org/en/corporate-surveillance> accessed 27 May 2018.

[98] Chapter 1, section 1.1.

[99] ENISA, 'Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems' (2015) 6.

[100] Herman T Tavani, 'KDD, Data Mining, and the Challenge for Normative Privacy' (1999) 1 Ethics and Information Technology 265. OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 144.

[101] Roger Brooks, 'Artificial Intelligence vs. Machine Learning vs. Data mining 101 - What's the Big Difference?' (*Guavas Blog*, 6 October 2017) <https://guavus.com/artificial-intelligence-vs-machine-learning-vs-data-mining-101-whats-big-difference/> accessed 14 June 2018.

[102] Bart HM Custers, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Wolf Legal Publishers 2004) 19.

[103] Galit Shmueli and others, *Data Mining for Business Analytics Concepts, Techniques, and Applications in R* (Wiley 2018) 20.

[104] Roger Brooks, 'Artificial Intelligence vs. Machine Learning vs. Data mining 101 - What's the Big Difference?' (Guavas Blog, 6 October 2017) <https://guavus.com/artificial-intelligence-vs-machine-learning-vs-data-mining-101-whats-big-difference/> accessed 14 June 2018. See more on machine learning in relation to profiling in Section 9.2.2.

[105] Bernard Marr, 'What Is The Difference Between Artificial Intelligence And Machine Learning?' *Forbes* (6 December 2016) <https://webcache.googleusercontent.com/search?q=cache:Qy4RIWTPArUJ:https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/+&cd=13&hl=en&ct=clnk&gl=us&client=safari> accessed 27 May 2018.

[106] Ian Kerr and Jessica Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65, 66.

of a 'big data prediction machine'.[107] Today, (predictive) data analytics occurs to a much greater extent and more easily compared to analytical endeavours in the past. This has been attributed to more extensive data gathering, the easier process of combining databases, and more powerful computer technologies to analyse the data.[108]

An example of sophisticated data analytics is ToyTalk, a US start-up company that operates the speech processing services for Hello Barbie and conducts analysis of the recordings of conversations between children and dolls.[109] ToyTalk's algorithm identifies sentences and phrases spoken aloud to the doll by converting them into text and analysing that text using the company's own application based on the knowledge gathered from Google Search, Wikipedia, and Weather Underground.[110] The technology enables the doll to respond to a child with lines of related, pre-recorded dialogue, adapted to every child's personal situation. With the help of analytics, Hello Barbie improves as a product, eventually increasing its value. However, abuses cannot be excluded. For instance, children's conversations could be mined to determine what products should be marketed to children and this information could be shared with advertisers.

2.3. How does the data-driven (big data) economy work?

The question critical to all commercial actors in the data economy is how to 'polish the data diamond' in the most profitable way. This leads to the topic of business models and strategies, which, in essence, describe ways in which companies use data to make money.[111]

This section aims to outline a high-level business model for data value creation to understand how the big data economy works and in what ways personal data is used. Of course, not all companies active on the data market follow the same strategy. Some of them are only involved in part of the process, and others choose their own strategy of value creation. However, for a typical data-driven business, the value creation model can be broken down into three key phases: 1) data collection, 2) data analytics and software, and 3) decision-making.

---

[107] Ibid., 67.

[108] Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477, 506. Also see Helen Nissenbaum (2010) 43.

[109] <https://www.toytalk.com/about/> accessed 3 October 2016.

[110] Ibid.

[111] A business model is a term used to describe the strategy for data collection and reuse on such a large-scale. It can be explained through the value chain approach. In the internet economy, it typically consists of two parts of activities: first, activities associated with making something such as design, purchase of raw materials, manufacturing, and so on. Second part of the chain represent the activities associated with selling something: finding and reaching customers, transacting a sale, distributing the product or delivering the service. Joan Margaretta, 'Why Business Models Matter' *Harvard Business Review (May 2002).*

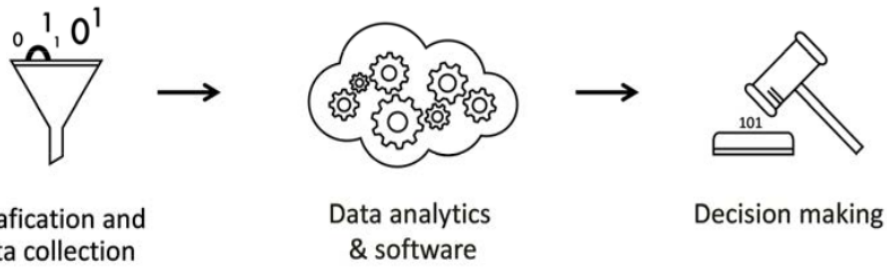

Figure 1: Data-driven value chain[112]

2.3.1. Data acquisition

The first issue that needs to be addressed is how data is generated and/or how it can be acquired. For obvious reasons, only examples of acquisition and generation of *personal* data are discussed here.[113] Although the list below is not exhaustive, it is broad enough to give an idea of the most common types of data collection and acquisition in the big data economy.

Data generating platforms such as Facebook, Google, and Strava are the most notorious collectors of personal data. These platforms generate data as a by-product of their actual business activity to support the sales of (digital) goods and services.[114] The main characteristic of service platforms is that they benefit from data enabling multi-sided markets.[115] On the one side of the market, platforms enter into relations with consumers by offering them free services; in exchange, they are able to capture a vast amount of these consumers' personal data. On the other side of the market, platforms contract with advertisers or other third parties that are willing to pay for the users' data captured by the platform.

Individuals' online activities are tracked beyond the activities of the data generating platforms. Features like IP addresses, authenticated logins, and cookies are exploited to monitor online behaviour.[116] Nowadays, almost every website is designed in a way that requires observing every visitor: time of visit, number of clicks, and moves across the screen. These activities represent only a part of all the personal data generated by the data economy but lie at the heart of many data-driven companies.[117]

Among indirect sources of personal data, *data brokers* are companies specialised exclusively in the provision of data. They compile personal data that comes from different suppliers and process it to enrich, clean, or analyse it.[118] The data is then provided to clients, such as social media and insurance companies. Typically, brokers' data is not sold but licensed.[119] Besides data brokers, data can also be

---

[112] Adapted from OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 132.
[113] Big amounts of non-personal data are generated as the by-product of an industrial activity. For instance, raw data collected by satellites or computer data generated in physics labs represents world's largest databases. Vivien Marx, 'The Big Challenges of Big Data' (2013).
[114] Cornelius Puschmann and Jean Burgess, 'The Politics of Twitter Data' in Katrin Weller and others (eds), *Twitter and Society* (Peter Lang Publishing, Inc 2014) 47.
[115] D. Daniel Sokol and Roisin Comerford, 'Antitrust and Regulating Big Data' [2016] Geo. Mason L. Rev. 1129, 1141.
[116] Nissenbaum (2010) 29.
[117] Ibid.
[118] Federal Trade Commission, 'Internet of Things: Privacy & Security in a Connected World' 3.
[119] <http://www.gartner.com/it-glossary/data-broker/> accessed on December 28, 2016.

acquired from commercial or non-commercial entities that generate data but are not willing or not able to reuse it in an innovative and profitable way. An example of data licensing (without any data broker being involved) is the agreement between the UK National Health Service (NHS) and Google DeepMind.[120] NHS owns a vast amount of medical data but has no capabilities to reuse it. Instead, it is interested in licensing or selling the data to someone with appropriate knowledge and technical capabilities. As a global leader in AI, Google is certainly a suitable partner.

Open data is gathered from publicly available records. Through open data initiatives, the public sector encourages access to and reuse of public data, including personal data. A recently founded public data distributor in the EU is the EU Open Data Portal, which provides access to large databases generated by EU institutions.[121] Open access to data is also offered by some private companies. Twitter, for instance, enables third parties to explore and reuse the data published on the platform.[122]

Machines and sensors that are part of the IoT generate a vast amount of data too.[123] Much of the data collected in the IoT environment relates, directly or indirectly, to individuals. As people are becoming more engaged with the technology, every aspect of their life is measured with sensors and analysed using big data analytics techniques. For example, radio-frequency identification (RFID) technology enables invisible monitoring of customers by tracking the tags of products that consumers put in their shopping carts.[124]

Finally, a *combination* of existing data sets is an additional way to acquire data. New data can be generated by analysing existing data, which in turn constitutes new personal data.[125] For example, after a user joins Facebook and consents to personal data processing, Facebook starts collecting vast amounts of her personal data. However, that is not all: the company combines these data sets with additional data purchased from data brokers to create a more precise picture of a user and to sell this enriched information to advertisers.[126]

From the perspective of an individual, data acquisition can be described as monitoring and tracking.[127] After all, every single visit to a website is registered by the website owner. Although visitors are typically asked to consent to the processing of personal data, tracking and monitoring can lead to subtle and disguised forms of data collection. These are rarely presented to the consenting individual in an informative and transparent way.

---

[120] Jane Wakefield, 'Google given access to London patient records for research' *BBC News* (3 May 2016) <http://bbc.com/news/technology-36191546> accessed 27 May 2018.
[121] <https://data.europa.eu/euodp/data/> accessed 27 May 2018.
[122] <https://developer.twitter.com/en/docs/tweets/search/overview> accessed 27 May 2018.
[123] See section 2.2.1.
[124] Article 29 Data Protection Working Party, 'Working Document on Data Protection Issues Related to RFID Technology' (2003).
[125] Manon Oostveen, 'Identifiability and the Applicability of Data Protection to Big Data' [2016] International Data Privacy Law 6.
[126] Evan Selinger and Brett Frischmann, 'Why it's dangerous to outsource our critical thinking to computers' *The Guardian* (10 November 2015) <https://www.theguardian.com/technology/2016/dec/10/google-facebook-critical-thinking-computers?CMP=Share_iOSApp_Other> accessed 28 December 2016. However, note that Facebook's CEO Mark Zuckerberg testified in 2018 that the company no longer uses this method of data enrichment. Transcript of the hearing of Mark Zuckerberg in the US Congress on April 10, 2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.013eea956ff1> accessed 28 May 2018.
[127] Also described as *dataveillance*. See for example David Lyon, 'Surveillance, Power and Everyday Life' in Robin Mansell and others (eds), *Oxford Handbook of Information and Communication Technologies* (Oxford Univeristy Press 2007).

When an individual is put at the centre, three categories of collected personal data can be distinguished:

(1) *Self-reported data,* or information that people volunteer about themselves, such as their email addresses, work and education history, and age and gender.[128] This often happens as part of a data generating platform activity. Examples include creating a social network profile and entering credit card information for online purchases.[129]

(2) *Digital exhaust,*[130] such as location data and browsing history, which is created when using mobile devices, web services, or other connected technologies.[131] In contrast to volunteered data, where the individual is actively and purposefully sharing his data, exhaust data can be generated even though a subject remains passive. This does not mean that digital exhaust is less useful or less revealing than self-reported data. In fact, the contrary can be true.[132]

(3) *Inferred data,*[133] or personal profiles used to make predictions about individual interests and behaviour, which are derived by combining self-reported data, digital exhaust, and other data.[134] An example is a consumer profile constructed by combining the RFID tags of the items purchased by a user and some other information about this specific consumer, e.g. her watch's RFID.[135] It is important to note that personal data can be also 'inferred' from pieces of 'anonymous' or 'non-personal' data.[136]

To determine how much consumers value their data, Harvard researchers examined the amount of money that survey participants would be willing to pay to protect different types of information.[137] The results showed that people valued self-reported data the least, digital exhaust more, and profiling data the most. Surprisingly, when it comes to legal protection of personal data, the order is not necessarily the same. Profiling data only recently received explicit and stronger protection under EU law.[138]

2.3.2. Data analytics and other software used to gain insights

The next step in the data value chain is the deployment of data analytics. From the business perspective, analytics is a segment of business intelligence that uses data tools to analyse and understand data. The task of analytics is to tailor data to draw useful actions and improve key performance indicators.[139]

---

[128] Timothy Morey, Theodore Forbath and Schoop Allison, 'Customer Data: Designing for Transparency and Trust' *Harvard Business Review* (May 2015).
[129] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being'.
[130] In the OECD terminology, this is *observed* data. I use the expression *digital exhaust* as it appears more illustrative.
[131] Morey, Forbath and Allison (2015).
[132] For example as metadata - data that provides information about other data. Merriam-Webster online dictionary <https://www.merriam-webster.com/dictionary/metadata> accessed 28 December 2016.
[133] Used by the OECD and Mireille Hildebrandt. See OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being'; Hildebrandt (2008).
[134] Morey, Forbath and Allison (2015).
[135] Article 29 Data Protection Working Party, 'Working Document on Data Protection Issues Related to RFID Technology' 6.
[136] OECD 'Data-Driven Innovation: Big Data for Growth and Well-Being' 152.
[137] Morey, Forbath and Allison (2015).
[138] In the upcoming GDPR, profiling data is explicitly protected under Article 20. See Chapter 9 for more details.
[139] Mayer-Schönberger and Cukier (2014).

The OECD distinguishes three main functions through which companies use data analytics to gain insights:[140]

(1) *Extracting information from unstructured data*. Unstructured data is by far the most frequent type of data but is hardly useful. To structure it in a predefined data model, different analytical techniques can be applied.[141] Modern analytics enables insights into databases that were not possible in the past. For example, a large collection of photos can be interpreted by using analytical software. One such well-known photo recognition algorithm has been developed by Facebook. This technology has given Facebook *'the ability, in a semantically appropriate way, to describe what's happening in a photo, that's very advanced and starting to approach the holy grail of image recognition.'*[142]

(2) *Digital real-time monitoring*. The fact that data is collected at a high speed and can be processed and analysed instantly represents a large benefit for the economy. By gaining real-time insights, companies are able to base decisions on evidence that is very close to the actual market situation (e.g., customers' current preferences, trends). Such monitoring may also benefit consumers. An illustrative example comes from the energy sector. BC Hydro is an electric utility providing power to nearly 2 million Canadian residents.[143] In 2011, the company began upgrading its electricity meters to smart meters. Users can now track their energy use per hour and see trends in their own usage data. As a result, it is easier for them to keep their use of energy and spending under control.

(3) Inference and prediction. Sophisticated data analytics supports data-driven inference and prediction. The discovery of knowledge is now possible even if there was no prior record of such information.[144] To use the example above, Facebook's face recognition algorithm is not only able to organise users' photos but also to automatically identify and tag users according to user-provided photos. Netflix, a data-driven company that collects information from its 50 million plus subscribers at an extraordinary speed, is known for its sophisticated predictive algorithm which is able to provide personalised movie suggestions to individual users.[145]

Appreciating the power of information to analyse people and to predict and even control their actions is nothing new. In fact, understanding and foreseeing human behaviour has always been a part of human social relations and interaction.[146] However, for the reasons explained above, it now occurs to a much greater extent. In fact, analytics represents an increasingly important aspect of the modern data economy. Some of the world's most successful and innovative companies, such as Google,

---

[140] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 150-153.
[141] See section 2.2.4. for some examples of analytical techniques.
[142] <http://digiday.com/platforms/facebooks-new-image-recognition-technology-data-windfall-advertisers/> accessed on December 28, 2016.
[143] Conner Forrest, 'Ten Examples of Iot and Big Data Working Well Together' *ZDNet* (2 March 2015) <http://www.zdnet.com/article/ten-examples-of-iot-and-big-data-working-well-together/> accessed 27 May 2018.
[144] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 36.
[145] A Porat and LJ Strahilevitz, 'Personalizing Default Rules and Disclosure With Big Data' (2014) 112 Michigan Law Review 1417, 1451-1452.
[146] Nissenbaum (2010) 43.

Facebook, Amazon, and eBay, have built their business model on the analytical exploitation of big data.[147]

In general, analysts are interested in trends, models, and correlations, and not in a specific individual. However, individuals can be greatly affected by the failures of the analytical processes when applied to them, e.g. the use of biased data.[148] Consider the following example. A company wants to create the ideal profile for its next top manager. On the basis of the available data, the algorithms discover that the ideal top manager is a middle-age white male. As the database probably contained many top managers with this profile, the resulting pattern only confirms the discriminatory tendency in the hiring processes.[149] These negative consequences escalate in the final stage of the data value chain, when data-driven decisions are made. Section 2.4.2. explores those risks in more detail.

2.3.3. Generating value through decision-making

The final step in the data value chain is acting upon discovered knowledge, i.e. using insights in data to draw useful decisions that generate value. This knowledge can either be a result of the analysis of a company's own data or it can be derived from a third party's data. The process of decision-making can be supervised by a human, but it can also run autonomously without any human interference.

Netflix, an American streaming media provider, serves as a model for decision-making based on internal data analysis. As mentioned above, Netflix uses sophisticated predictive algorithms that are able to provide personalised movie suggestions to individual users. This specific knowledge of users' movie preferences also drives the company's business decisions. By observing that subscribers who watched the original British version of House of Cards were highly likely to watch movies starring Kevin Spacey or directed by David Fincher, the company predicted the success of the new House of Cards series. Eventually, the company started licensing the series, which was a great success and brought it a large profit.[150]

Decision-making that is based on multiple input is typical to the field of behavioural targeting. An advertising network follows an Internet user's behaviour while he surfs the Web. Different technologies enable the tracking of consumers, but typically *'cookies are used […] to identify users who share a particular interest …'*.[151] By knowing users' shopping preferences, the network is able to create customer profiles and provide each user with an individually targeted advertisement. Ad networks' insights are utilised by advertisers to target consumers with more relevant ads.

An example of a more complex yet promising strategy of profit generation is the agreement between Google and the NHS. The agreement has allowed Google to access about 1.6 million patient records.[152] Google's AI division DeepMind will use the data to develop an early warning system for patients at risk

---

[147] Fortune 500 list for 2016 shows the world's most successful companies. Data-driven companies top the list – Walmart is on the first and Apple is on the third place <http://fortune.com/fortune500/> accessed 24 January 2016.
[148] Oostveen (2016) 7.
[149] Bart Custers and Helena Ursic, 'Worker Privacy in a Digitalized World under European Law' 39 Comparative Labor Law & Policy Journal 323.
[150] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 152-153.
[151] Frederik Zuiderveen Borgesius, 'Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 Computer Law & Security Review 5.
[152] Jane Wakefield, 'Google given access to London patient records for research' *BBC News* (3 May 2016) <http://www.bbc.com/news/technology-36191546> accessed 27 May 2018.

of developing acute kidney injuries.[153] Insights will be also used by hospitals to streamline and improve health treatments.[154]

The idea of Google as the NHS health data user has triggered much public disapproval for reasons concerning possible interference with collective and individual rights. Some have criticised the fact that a vast amount of data was transferred to Google with such ease, and pointed at the long-lasting relevance of knowledge that might be hidden within the set.[155] That discussion partly explains why the third step in the data value creation model matters from the individual perspective. However, data-driven decisions also have some short-term consequences. For example, Netflix has mastered the ability to identify and recommend movies that keep us attached to its service.

What is also relevant from an individual point of view is the automatisation of decision-making. More and more decisions are made without any human involvement.[156] While automatisation has a great potential for the economy, it also opens some difficult issues related to the protection of individuals. Some concerns regarding non-transparency and power asymmetries are explored in sections 2.4.2.2. and 2.4.2.4.

2.4. The individual in the data-driven economy

A vast amount of information in the digital universe is created by *individuals,* including phone calls, emails, photos, online banking transactions, and postings on social networking sites such as Twitter.[157] Moreover, data generated by machines or combined from several sources can, directly or indirectly, be related to an individual person.[158]

Every online appearance leaves a digital trace, which gradually grows into a vast registry of the actions constituting 'data doubles' or 'quantified selves'.[159] By participating in these activities, individuals actively contribute to and co-create the data economy. As shown above, this data represents the raw material for the entire online service industry.

The fact that personal data sources are highly interesting and useful in the data economy has led to their commodification and commercialisation. Commodified personal data is a discrete package of personal information that can be exchanged for something else.[160] Using data as an object in a business exchange creates (monetary) value. However, by taking the form of a commodity, personal data is devaluated to the level of a commercial good. For a concept that has been granted human rights protection, this is a delicate transformation.[161]

---

[153] Ibid.
[154] Ibid.
[155] Julia Powles and Hal Hodson, 'Google DeepMind and Healthcare in an Age of Algorithms' (2017) 7 Health and Technology 351.
[156] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 145-155.
[157] Conner Forrest, 'Ten Examples of lot and Big Data Working Well Together' *ZDNet* (2 March 2015) <http://www.zdnet.com/article/ten-examples-of-iot-and-big-data-working-well-together/> accessed 27 May 2018.
[158] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2017) 14 <https://ssrn.com/abstract=3083554> accessed 28 May 2018.
[159] Gemma Galdon Clavell, 'Policing, Big Data and the Commodification of Security' in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 106.
[160] Paul Schwartz, 'Property, Privacy and Personal Data' (2003) 117 Harvard Law Review 2056, 2069.
[161] See Chapter 3 on data protection law and its constitutional roots.

In estimating the impacts of the data economy on individuals, authors in the economic field seem to contradict each other. Some believe that data can play a significant economic role to the benefit of both private commerce and national economies and see a great benefit of the data-driven economy for the well-being of citizens.[162]

In contrast, others warn that an expanding consumer surplus means that many producer surpluses have been competed away.[163] In other words, the data-driven economy largely benefits individuals and leaves commercial actors worse off. However, a third stream of economists believe that the big data economy in fact decreases consumer surplus.[164] Their argument is in line with those who question data economy benefits due to decreasing privacy protection, discrimination, and other negative implications.[165]

Preceding sections have already indicated that data exchange carried out on the Internet is not only innocent and advantageous. Several risks of data-driven business processes have already been briefly mentioned: non-transparent data tracking and monitoring, decreased control over data stored in the cloud, and inexplicability of algorithms.

As the data-driven economy is becoming more influential, gains and opportunities need to be carefully balanced. This requires a trade-off between big data risks and rewards. In fact, striking the right balance could be one of the greatest public policy challenges of our time.[166]

2.4.1. Benefits

Taking part in the data economy has the potential to enhance an individual's overall well-being. The term well-being is understood as a combination of social, economic, and psychological states associated with positive feelings.[167] Four groups of benefits that enhance well-being are described shortly below. The list is not exhaustive because it only clusters those that are most commonly observed. Not only individual benefits but also positive outcomes of data processing for society as a whole are taken into account.

2.4.1.1. Convenience

Sharing personal data can be convenient. For example, most people prefer to use a credit card rather than a debit card for the convenience of a deferred payment, although this eventually decreases the confidentiality of their purchases.[168] In a similar vein, when someone agrees to share data with advertisers, she is alerted about relevant offers and redirected to the most relevant product.

---

[162] McKinsey, 'Big Data: The next Frontier for Innovation, Competition, and Productivity' 1-2. Also see OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being'.
[163] Brian Kahin, 'Digitization and the Digital Economy' (2013) <http://ssrn.com/abstract=2782906> accessed 27 May 2018.
[164] Anna Bernasek and DT Mongan, *All You Can Pay* (Nation Books 2015).
[165] See for example Tal Z Zarsky, '"Mine Your Own Business!": Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion' (2002) 5 Yale Journal of Law and Technology 1306.
[166] Lynskey (2015) 202.
[167] For the definition of well-being see Carol D Ryff 'Happiness is everything, or is it? Explorations on the meaning of psychological well-being' [1989] 57 Journal of personality and social psychology 1069.
[168] Kent Walker, 'Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange' (2000) 190 Stanford Technology Law Review 1.

Withholding contact information typically results in limited availability (or unavailability) of the discounts and offers such as free videos, discounts on children's toys, or cut-rate airfares.[169]

2.4.1.2. Self-expression and self-control

With recent technological advances, personal data may also become a way of self-expression leading to one's own (representation of) identity.[170] For instance, the Strava app has created a large 'quantified self-movement' community.[171] Users who track their sport activities are encouraged to share and analyse results on the platform. Large-scale data collection and real-time aggregation of data give them an opportunity to monitor their training, compare it against that of other peers, and challenge themselves by setting higher goals.

The quantified-self apps often offer functions beyond fitness tracking. For instance, women trying to conceive use apps to track their periods, basal temperature, weight, mood, and sex life.[172] If they feed the app with enough data, the algorithm is able to calculate their ovulation date and assess their chance of pregnancy.

2.4.1.3. Reduced cost and/or (in)direct monetary benefits

The use of personal data reduces marketing and distribution costs for both businesses and consumers, and thus ultimately decreases the prices of all goods and services.[173] Targeted offers help sellers avoid investing time and resources in targeting uninterested buyers, which translates to a better price for those who do actually show interest in the products.

SkyScanner's search algorithm proves that a company's successful data-driven service can directly benefit consumers.[174] SkyScanner is a global metasearch engine for information on the World Wide Web that enables people to find comparisons for flights, hotels, and car hire services. It gathers data from numerous airliners and comes up with a selection of the most affordable flights based on the user's preferences. Those who use the service agree that it makes life much easier and are reluctant to abandon it.[175]

The technological revolution driven by big data has the potential to empower individuals even more profoundly. Since Web 2.0 emerged, users have been given exciting opportunities to take a more active role on the Internet.[176] Today, consumers no longer passively observe the online market, but actively engage in the economic exchange. An empowered and more independent consumer can instantly move between the two poles of consumption and production. Airbnb is a platform which, with the help of big data, connects property owners with those searching for short-term accommodation. By using Airbnb's big-data-driven service, an owner can effortlessly transform into a quasi-commercial

---

[169] Ibid.
[170] Michiel Rhoen, 'Beyond Consent: Improving Data Protection through Consumer Protection Law' (2016) 5 Internet Policy Review.
[171] <https://www.strava.com> accessed 27 May 2018.
[172] <https://itunes.apple.com/us/app/glow-ovulation-period-tracker/id638021335?mt=8> accessed 27 May 2018.
[173] Walker (2000) 8.
[174] Rubinstein (2013).
[175] Skyscanner was one of Scotland's most highly valued start-ups. The company has grown exponentially since it was set up in 2003. Steve Vance, 'Skyscanner acquired by Chinese travel giant Ctrip in a £1.4 billion deal' *Citya.m.* (19 September 2016) <http://www.cityam.com/248684/significant-investment-puts-skyscanner-firmly-position> accessed 27 May 2018.
[176] Daly (2016).

party with access to the global market. Not only does this reduce the owners' cost, it also opens up possibilities for direct monetary benefits.

Furthermore, some assert that individuals should be free to derive some direct benefit, including monetary, from the use of their personal data.[177] Personal datasets could be licensed to third parties in exchange for additional services, e.g. free social networking, or for cash value.[178] In some sense, this is already happening. The notions of economic value and ownership of personal data are a reality of modern data processing practices.[179] However, full application of the property law regime to personal data[180] is probably not feasible under the current legislation,[181] nor is it in line with the European fundamental rights doctrine, which perceives protection of data as an unalienable right.[182]

2.4.1.4. New knowledge and innovations

Data collected via various media – Internet, communication, cameras – works as an asset and raw material for commercial actors in the data economy and for science and society at large. Patterns of behaviour identified on the group level can have long-reaching consequences. In the healthcare sector, platforms constructed based on data from millions of patients and their health records have the potential to revolutionise clinical research and to bring significant benefits to many stakeholders, including patients, health systems researchers, industry, and society.[183] An example is the Dutch start-up Filterless, which has developed software to combine millions of health data (mostly genome) collected by hospitals, insurance companies, and pharmaceutical companies, and mine it with the goal of finding new insights that could help healthcare providers improve treatments for all patients.[184]

Two conditions must be met to generate data-driven insights. First, individuals have to share their data. The technology's value increases with the number of people who use it or permit their information to be shared. Sharing customer data on a large scale creates a consumer community where each participant can benefit from the experience and information of a fellow customer. For instance, Amazon recommends additional books that users might like based on the purchasing patterns of others who have bought the same books in the past.[185] Had all fellow users refused to provide a recommendation, assessing a book's suitability would become much more difficult and costly. Walker contends that certain socially beneficial products and services can only exist if everyone agrees to participate, and calls the opposite situation a 'tragedy of commons' that can best be illustrated with a phone directory: unless the majority of people agree to share information, the directory is useless.[186]

---

[177] See for example Lessig (2006) 228.
[178] European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014).
[179] Nadezhda Purtova, 'The Illusion of Personal Data as No One 's Property' (2015) 7 Law, Innovation and Technology 83, 4.
[180] E.g. using a license to perform an infinite transfer of personal data from an individual to a commercial entity.
[181] See for example EU Charter, Article 8.
[182] See for example: European Court of Human Rights, Sanles Sanles v. Spain, app.no. 48335/99; European Court of Human Rights, Thévenon v. France, app.no. 2476/02; European Court of Human Rights, Mitev v. Bulgaria, app.no. 42758/07; European Court of Human Rights, M.P. and Others v. Bulgaria, app.no. 22457/08; European Court of Human Rights, Koch v. Germany, app.no. 497/09.
[183] P Coorevits and others, 'Electronic Health Records: New Opportunities for Clinical Research' (2013) 274 Journal of Internal Medicine 547.
[184] <http://filterless.nl/index.php/drug-discovery/> accessed 27 May 2018.
[185] Walker (2000) 14.
[186] Ibid., 12.

The second condition for knowledge generation and innovation is openness of data. This is why policy-makers strongly encourage governmental data sharing. The objective is to reuse data and accrue value for businesses and for citizens. One good practice comes from Chicago, where the municipal open data platform supported app developers to build innovative solutions based on public data. For example, developers created an interactive map that lets citizens find out how a building is zoned, learn where to locate a business, or explore zoning patterns throughout the city.[187] Due to many positive side effects such as transparency, increased trust, and added value, EU member states are required to make as much public information available for reuse as possible.[188]

2.4.1.5. Security of data and citizens

With more data available and processed, it is growing increasingly difficult to disguise someone's identity. This in turn means better security, as fraudulent individuals and entities can no longer take part in the digital market.[189] Furthermore, being able to assess vast amounts of data to identify suspicious incidents can help identify criminal behaviour and prevent costs. Palantir, a US software company, has been selling its big data tools to the police and government departments to flag traffic offenses, parole violations, and other everyday infractions.[190] Palantir's software can ingest and sift through millions of digital records across multiple jurisdictions, spotting links and sharing data to make or break cases. The police have neither the technical resources nor sufficient data to carry on such an analysis themselves.[191] For better or worse, the police departments that deploy Palantir have become dependent upon it for some of their most sensitive work.

2.4.2. Risks

Big data is a recent, evolving phenomenon. As a consequence, many of its risks are yet to be explored. In addition, because big data activities are often carried out in disguise and are highly complex, the risks are difficult to notice.

Therefore, it is impossible to provide an exhaustive list of big data risks. Instead, the analysis should focus on a limited number of core values that can be compromised as a result of big data business practices. To tackle this task, the following sections build on Richards and King's framework of three paradoxes of big data: the transparency, the identity and the power paradox.[192] These paradoxes elucidate the values that can be undermined by the growing big data economy: privacy, transparency, autonomy, and power symmetry.

---

[187] <https://secondcityzoning.org> accessed 27 May 2018.
[188] 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 [2013] OJ L175/1.
[189] The danger is, however, that the state's concerns for security can be turned into undesirable surveillance. For example, China recently introduced a social credit scoring system based on citizens' behavior on social networks. See for example Rachel Botsman, 'Big data meets Big Brother as China moves to rate its citizens' (*21 October 2017*) <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> accessed 27 May 2018.
[190] Mark Harris, 'How Peter Thiel's Secretive Data Company Pushed Into Policing' *Wired* (8 September 2017) <https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/> accessed 27 May 2018.
[191] Ibid.
[192] Neil M Richards and Jonathan J King, 'Three Paradoxes of Big Data' (2013) 66 Stan. L. Rev. Online.

2.4.2.1. Compromised privacy

Privacy is a concept that allows for multiple definitions.[193] Chapter 3 of this thesis provides a detailed analysis of the term and traces back attempts to capture its meaning. For now, it suffices to understand privacy in its ordinary sense: as an attribute of things that affect or belong to private individuals, that are generally distinct from the public, and that are kept confidential and secret (e.g. not disclosed to others and kept from public knowledge or observation).[194]

The data-driven economy often gives the impression that privacy has been eliminated or is even dead.[195] Mark Zuckerberg, Facebook's CEO, argued that privacy has fundamentally evolved in recent years and can no longer be seen as a social norm.[196] While it is true that privacy as a social norm has been transformed, it has not lost any of its strength. On the contrary, considering the many new types of privacy violations, some of which are mentioned below, privacy has never been more relevant. Zuckerberg himself is proof. In a photo shared via Twitter in the summer of 2016, his computer can be seen, on which the camera and headphone jack are covered with tape, and the email client he uses is Thunderbird (a popular email client among the tech-savvy, and particularly those who want to use PGP-encrypted emails).[197] Zuckerberg's example may sound anecdotal but it is an indicator of a wider trend, suggesting that people increasingly care about keeping his work and conversations private.

In the data-driven economy, dataveillance is what most apparently puts privacy at risk. Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.[198] In the data economy, in which individuals' behaviour and all their actions are increasingly datafied, dataveillance is easy to conduct. Clarke observes that it is significantly less expensive than physical and electronic surveillance, because it can be automated. As a result, the economic constraints on dataveillance are diminished, and more individuals, and larger populations, can be monitored.[199] Dataveillance can be particularly dangerous because it enables the inference of facts that someone would rather keep secret. For example, a person shares information about her hobbies or favourite books but not information about her sexual orientation. However, by using big data techniques, this information can be predicted anyway. Kosinski, Stillwell, and Graepel have shown how a range of highly sensitive personal characteristics, including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, and parental separation, can be predicted highly accurately on the basis of Facebook likes.[200] Connected devices are another example of how big data quickly escalates into riskier conduct. IoT enables easy integration, aggregation, or correlation of various aspects of users' identity.[201] At first glance, this gathering of data is just a step in the data-driven value chain (data

---

[193] Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1088.
[194] The Concise Oxford dictionary (1990), Black's Law Dictionary (1910).
[195] Neil M Richards and Jonathan J King, 'Big Data Ethics' (2014) 49 Wake Forest Law Review 393, 409.
[196] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' (10 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 27 May 2018.
[197] Katie Rogers, 'Mark Zuckerberg Cover His Laptop Camera. You Should Consider It, Too.' *The New York Times* (22 June 2016) <https://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html> accessed 14 June 2018.
[198] <http://www.rogerclarke.com/DV/Intro.html#Priv> accessed 3 October 2016.
[199] <http://www.rogerclarke.com/DV/Intro.html#Priv> accessed 3 October 2016.
[200] M Kosinski, D Stillwell and T Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110 Proc Natl Acad Sci USA 5802.
[201] Kord Davis, *Ethics of Big Data* (O'Reilly Media, Inc 2012) 33.

acquisition). However, it may lead to disclosure of some highly sensitive details.[202] For instance, electronic toothbrushes may reveal how often and how long people brush their teeth, indicating potential health issues.[203]

In the big data economy, even anonymised data cannot guarantee privacy. In fact, anonymised data can be as useful as personal data in many cases.[204] A typical example is a company that wants to personalise its marketing campaigns with the help of profiling. The use of personal data may be helpful to assess which people are potentially interested in particular products or services, but aggregated data on the street or neighbourhood level may be similarly useful and cheaper to process. Inferring information from group profiles supports predictions about someone's personal circumstances. As soon as '*[t]hree or four data points of a specific person match inferred data (a profile), which need not be personal data […]',*[205] a company is able to highly accurately predict characteristics of individual users.[206]

The flow of data among the actors in the data-driven economy escalates the risk of privacy intrusions. This is why Nissenbaum believes that meeting individual expectations about the flow of personal information sits at the core of privacy.[207] The section on data acquisition mentioned a number of data sources, including data brokers. Specifically, it pointed to the fact that data is often acquired by means of data combination. For example, Facebook's own databases are merged with detailed dossiers obtained from commercial data brokers about users' offline life.[208] In this way, Facebook improves its own data with categories that users did not share or want to reveal on Facebook. If information is used in contexts that are at odds with individuals' expectations, this can lead to feelings of awkwardness and discomfort.[209]

2.4.2.2. Lack of transparency

Transparency describes something that is easy to perceive or detect, and is open to scrutiny. In contrast, non-transparency can be illustrated with the metaphor of a black box: a complex system or device whose internal workings are hidden or not readily understood.[210] In the context of data-driven decision-making, the black box metaphor stands for outcomes that emerge without satisfactory explanation.

Transparency is the second value at risk in the era of the data-driven economy. Although big data promises to make the world more transparent, its collection is invisible and its tools and techniques

---

[202] Custers and Ursic, 'Worker Privacy in a Digitalized World under European Law' 330.
[203] Ibid.
[204] Daniel Bachlechner and others, 'WP1 Mapping the Scene: D1.2 Report on the Analysis of Framework Conditions (Deliverable for the EuDEco H2020 Project)' (2015) 30 <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/d1.2_analysisoframeworkconditions-v1_2015-08-31-1.pdf> accessed 14 June 2018.
[205] Hildebrandt (2013) 33.
[206] Porat and Strahilevitz (2014) 1440.
[207] Nissenbaum (2010).
[208] Julia Angwin, Terry Parris Jr. and Surya Mattu, 'Facebook is quietly buying information from data brokers about its users' offline lives' *Business Insider* (30 December 2016) <http://www.businessinsider.com/facebook-data-brokers-2016-12?r=UK&IR=T> accessed 14 June 2018.
[209] Nissenbaum (2010) 21.
[210] <https://en.oxforddictionaries.com/definition/black_box> accessed on 9 January 2017.

opaque, curtained off by layers of physical, legal, and technical protection.[211] Non-transparent processing of data occurs in all three stages of the data-driven value chain: when data is acquired, when it is analysed, and when it is used. To illustrate the problem, three examples are given below: privacy policies, algorithmic black box, and the cloud computing black box.

Privacy policies (notices). The ubiquitous and automated collection of data in the data-driven economy is by definition opaque. Law requires data collectors to draft privacy policies to explain in what ways and under what circumstances personal data is collected, used, and shared. However, it has been shown that the objectives of privacy policies are flawed as people cannot understand the complex legalistic language, and policies are not specific enough to plausibly present what an individual actually consents to.[212]

Algorithmic black box. To extract useful patterns and create profiles, enormous amounts of consumer data are mined using complex algorithms.[213] As Pasquale points out, the key problem is that little is known about data mining and subsequent choice architecture processes.[214] In spite of being increasingly used to derive all sorts of findings, hidden algorithms are shrouded in secrecy and complexity. Barely anyone is able to fully capture how algorithms work and to monitor their actions. For example, Acxiom, the online data marketplace, is used as a source of numerous data points for an algorithm to determine a customer's creditworthiness.[215] Because of a bad credit score calculated on the basis of aggregated information, a consumer will be charged more, but she will never understand how exactly this amount was calculated or know what information Acxiom provided.[216] In addition, not even engineers working with the algorithms are fully able to capture their nature and monitor their actions.[217]

Cloud computing black box. The black box problem is duplicated in the cloud computing environment, mainly due to indefinite and non-transparent storage. In most cases individuals are unaware of what actually occurs in a cloud. Data can be shared with third parties, sold to advertisers, or handed over to the government. The loss of transparency on the Internet results in the feeling of powerlessness. As Schneier puts it, *'trust is our only option. There are no consistent or predictable rules. We have no control over the actions of these companies. I can't negotiate the rules regarding when yahoo will access my photos on Flicker. I can't demand greater security for my presentations on Prezi or my task list on Trello. I don't even know the cloud providers to whom those companies have outsourced their infrastructures […]. And if I decide to abandon those services, chances are I can't easily take my data with me.'*[218]

---

[211] Richards and King (2013) 42.
[212] Simone van der Hof, Bart W Schermer and Bart HM Custers, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies' (2014) 6 Policy and Internet 11.
[213] On the definition of profiling see Custers (2014) 156.
[214] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).
[215] See for example Mikella Hurley and Julius Adebayo, 'Credit Scoring in the Era of Big Data' (2016) 18 Yale Journal of Law and Technology 148, 175.
[216] Ibid.
[217] '... *even those on the inside can't control the effects of their algorithms. As a software engineer at Google, I spent years looking at the problem from within* …' David Auerbach, 'The Code We Can't Control' *Slate* (14 January 2015) <http://www.slate.com/articles/technology/bitwise/2015/01/black_box_society_by_frank_pasquale_a_chilling_vision_of_how_big_data_has.html> accessed 27 May 2018.
[218] Bruce Schneier, *Data and Goliath* (WWNorton & Company 2015) 115.

2.4.2.3. Undermined autonomy

Faden and Beauchamp define autonomy in practical terms as *'the personal rule of the self by adequate understanding, while remaining free from controlling interferences by others and from personal limitations that prevent choice.'*[219] Three dimensions of autonomy stem from this definition: self-governance (control), freedom from interference of others, and free choice. The examples below show how big data undermines each of them.

Free choice can be restricted as a result of limited confidentiality and privacy of personal data traces on the Internet. Knowing that the US National Security Agency (NSA) can follow every move we make might deter us from using a US online service.[220] The abstention from an action or behaviour due to the feeling of being observed is described as a *chilling effect*.[221] However, in some cases, the feeling of being watched creates a *nudge* for individuals to act. For example, research has shown that people pay more for coffee on the honour system[222] if eyes are depicted over the collection box.[223] Individuals' attitudes and behaviours change in such circumstances even though no real person is there. In 2009, German politician Malte Spitz sued a mobile network operator to obtain access to his mobile phone data. He then passed the information to Zeit Online, a news website, which created a visualisation showing where he had been and what he had been doing.[224] His profile was strikingly detailed, showing when Spitz had walked down the street, when he had taken a train, when he had been in an airplane, and where he had been in the cities he had visited. It also showed when he had worked, when he had slept, when he could have been reached by phone and when he had been unavailable, when he had preferred to talk on his phone, and when he had preferred to send a text message. It even showed which beer gardens he had visited in his free time.[225] Let us assume for the moment that these visits were not just frequent but rather excessive. If politician Spitz had known that someone could track his weekend visits to the beer gardens, would he still have been such a regular visitor, or would he have chosen a more neutral spot to spend his free time?

Another example of compromised autonomy is linked to non-transparent data processing and decision-making. In 2009, Eli Pariser noted that the news he received and search results that appeared on Google differed substantially from those viewed by his colleagues.[226] He soon realised that the reason was his personalised news website. Namely, based on his user profile and corresponding group profiles, the website was able to learn about his inferred political interests, which in turn meant that it could give more prominence to his favourite political group's media items. He described the situation

---

[219] Quoted in: Bart W Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent' [2013] Ethics & Information Technology 6.
[220] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books, 2014).
[221] Jonathon W Penney, 'Chilling Effects : Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Technology Law Journal.
[222] A system of payment or examinations which relies solely on the honesty of those concerned.
[223] Ryan M Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law Journal 1131, 1147.
[224] Dan Smith, 'Why can't we see the personal data we produce?' *The Telegraph* (5 July 2013) <http://www.telegraph.co.uk/sponsored/technology/technology-trends/10161697/personal-data.html> accessed 28 May 2018.
[225] Kai Biermann, 'Betrayed by our own data', *Zeit Online* (10 March 2011) <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz> accessed May 28 2018.
[226] Eli Pariser, 'Beware Online Filter Bubbles' *TedX Talk* (March 2011) <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en> accessed 3 October 2016.

as a *filter bubble*: *'a synonym for a unique universe of information for each of us.'*[227] The filter bubble represents the risk of seriously limiting someone's free choice. For example, when users of such personalised services form their political ideas, they may encounter fewer opinions or political arguments.[228]

2.4.2.4. Power asymmetries

In the data-driven economy, power is linked to two dimensions: 1) the access to data and control over it, and 2) the ability of sophisticated data processing.[229] The power asymmetry is most apparent in the relationship between data-driven businesses and individuals. However, it can also be observed in relationships between other actors in the economy. Small businesses often become dependent on and powerless in relation to big data holders.[230] Finally, power asymmetry affects authorities too, as they struggle to understand the data-driven economy and its consequences. '*[T]o understand what is going on we have to go for geeks,'* stated the director of the European Consumer Organisation to express her frustration with the data economy black box.[231]

To a large extent, the asymmetry between data controllers and individuals stems from the architecture of the data-collecting platforms. Because of these platforms' design, it is easy for them to take full ownership of users' input, e.g. photos, comments, and texts. In such circumstances, users' control over data fades away. Until recently, users of the dating app Tinder were asked to give away control of their pictures, videos, and chat logs forever.[232] Although individuals certainly benefit from the digital economy, e.g. by being able to use the Amazon online shopping tool, they pay (often unknowingly) for these services with their non-monetary assets, and their input is not always fairly evaluated.[233] In addition, the architecture of the platforms disables transparency. As explained above, algorithms that drive the functioning of the platforms are shrouded in secrecy and complexity, and barely anyone is able to fully capture how they work.

---

[227] Ibid.

[228] Filter bubble could even interfere with collective goods such as democracy. Harvard Law professor Jonathan Zittrain explained in 2010 how *'Facebook could decide an election without anyone ever finding out',* after the tech giant secretly conducted a test in which they were able to allegedly increase voter turnout by 340,000 votes around the country on election day simply by showing users a photo of someone they knew saying "I voted". Trevor Timm, 'You may hate Donald Trump. But do you want Facebook to rig the election against him?' *The Guardian* (19 April 2016) <https://www.theguardian.com/commentisfree/2016/apr/19/donald-trump-facebook-election-manipulate-behavior> accessed 28 May 2018. See also Robert M Bond and others, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489 Nature 295.

[229] Mark Andrejevic and Kelly Gates, 'Big Data Surveillance: Introduction' (2014) 12 Surveillance & Society 185, 190.

[230] For example, small business have limited access to many valuable databases. Bart Custers and Daniel Bachlechner, 'Advancing the EU Data Economy: Conditions for Realizing the Full of Potential of Data Reuse' (forthcoming in 2018) *Information Policy* 10-11.

[231] Monique Goyens, director general of the European Consumer Organisation, Welcome speech at the EDPS-BEUC conference (Brussels, 29 September 2016) <https://edps.europa.eu/data-protection/our-work/publications/events/edps-beuc-conference-big-data-individual-rights-and_de> accessed 28 May 2018.

[232] In March 2016, the Norwegian Consumer Council filed a complaint with the Norwegian regarding unfair contractual terms in the Terms of Use for the mobile application Tinder. As a result, Tinder later amended the disputable parts of the terms. David Meyer, 'Tinder Is in Trouble Over Its "Unfair" User Terms' *Fortune* (3 March 2016) <http://fortune.com/2016/03/03/tinder-norway-trouble/> accessed 28 May 2018. For a more detailed analysis of Tinder and other apps' terms by the Norwegian Consumer Council see Forbrukerrådet, 'Appfail? Threats to Consumers in Mobile Apps' (2016).

[233] Aleks, Jakulin (@aleksj), 'Why let Google show excerpts of your content in their search results without partaking in the lucrative search advertising revenue?' *Twitter* (April 29, 2016) <https://twitter.com/aleksj/status/725998664687206400> accessed 26 May 2018.

The asymmetry becomes even more apparent when personal data is processed as part of decision-making. Data controllers are able to leverage the collected personal data when they make commercial decisions, whereas individuals have little overview of the process. For instance, based on a personal data analysis, employers are able to determine employees' performance scores. As a consequence, individuals may face a lower salary or a risk of being fired.[234] Because such decisions are typically made on a multi-factor and multilevel analysis of workers' data, an individual may have trouble identifying what exactly is included in this performance that leads to such a 'verdict'.[235]

2.4.2.5. Discrimination

The key objective of *data-driven decision-making* is to differentiate between individuals. Clearly, such decisions can have important consequences for individuals and can work to both their advantage and disadvantage. Certain practices are legally allowed, though it could be argued that they are ethically disputable. For example, some online platforms are able to use the information collected by consumers to their disadvantage: by setting the price as close as possible to the maximum price that someone is willing to pay, they are able to exploit consumers' price sensitivity.[236] This is an example of price discrimination, which may become increasingly aggressive given the level of dataveillance on the Internet.[237]

However, data-driven decisions can also lead to *discriminatory practices* that cross the boundaries of what is legally acceptable. Discrimination that occurs when people are treated differently on the basis of protected grounds is prohibited regardless of whether it happens in a direct or indirect way.[238] An employer may refuse a candidate because an Internet (social media) search reveals how old she is. She may be in her 60s, and therefore too close to retirement, or she may be in her 30s, and therefore too likely to become pregnant. This would constitute illegal discrimination on the grounds of age or sex.[239] Data-driven decision-making may also lead to hidden discrimination. Group profiles inferred from big data are often used as a tool to make decisions about the members of the group, but not every group characteristic can justify different treatment. Characteristics such as address code can be legitimate factors according to which to differentiate, but they might mask ethnicity or religion – both of which are protected grounds.[240]

2.5. Conclusions

Chapter 2 answered the first research sub-question regarding the rise of the data-driven economy and the consequences for individuals. The chapter demonstrated that the world has entered a new era. Data-driven technologies and data analytics have spread across the economy, penetrating even some of the most traditional industries. In this growing data economy, personal data is treated as a highly valuable source, giving the data-driven firms a competitive edge. Individuals too have profited from

---

[234] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] International Data Privacy Law.
[235] Custers and Ursic, 'Worker Privacy in a Digitalized World under European Law' 340.
[236] Bernasek and Mongan (2015).
[237] Price discrimination and price differentiation are synonyms in economic jargon.
[238] Francesca Bosco and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (2015) 19.
[239] Lynskey (2015) 199.
[240] Custers (2004) 114.

the developments in technology: the prices of certain products have dropped; ordinary consumers have gained access to some sophisticated innovations; and the use of data has improved their lives. However, the intense personal data use has had some negative consequences such as privacy violations, information asymmetries, and imbalance of market power. As these harmful effects have not yet been fully explored, it is important that they are balanced carefully together with the positive outcomes of the data economy. Indeed, the profitable nature of data processing always has a reverse side, namely the need for better protection of personal data. This puts some limitations on what the industry can and cannot do, and law has an important role in setting the right boundaries. The following chapter provides an overview of some key legal rules that apply to the processing of personal data. Subsequently, the thesis is narrowed down to legal provisions that are addressed directly to individuals and concerned with (the extent of) their control over personal data.

3. SAFEGUARDING INDIVIDUALS IN THE DATA-DRIVEN ECONOMY – LEGAL FRAMEWORK[241]

3.1. Introduction

To answer the second research sub-question, '*What is the relevant EU regulatory framework for the data-driven economy from the perspective of an individual?',* Chapter 3 undertakes a study of applicable EU rules. As Chapters 1 and 2 explained, the developments in the data-driven economy put individuals at risk. Privacy intrusions, subtle forms of discrimination, limited autonomy in relation to personal data, and power asymmetries on the data-driven markets are some of the notorious threats. They can occur at different points in the data value chain, either at the moment of data collection, during the processing of data, or at the point when a data-driven decision is made.

To restore balance among the actors in the data-driven economy, the EU legal framework contains safeguards in the form of human rights instruments and secondary legal rules. These rules, which enhance individual protection in the data-driven economy, appear to be in disarray. To bring some order, this chapter systematically analyses the applicable legal provisions. The chapter is organised into two parts: section 3.2. focuses on EU primary law, in particular on the relevant human rights provisions, while section 3.3. relates to secondary legal provisions.

EU primary law refers to the body of treaties which represent the agreement of the EU member states and form the foundation of the EU.[242] Since the adoption of the Charter of the Fundamental Rights of the European Union (EU Charter) in 2009, human rights have occupied a central position within the EU (primary) legal order.[243] In the following section, eight human rights and freedoms are analysed from the perspective of the protection of individual and personal data in the data-driven economy: the right to privacy, the right to data protection, the prohibition of discrimination, the freedom of expression, the right to consumer protection, the right to do business, human dignity, and the rule of law.

Section 3.3. turns to EU secondary law. Secondary law is a specific manifestation of more general fundamental principles of EU law.[244] It comprises unilateral acts such as regulations and directives that enable the EU to exercise its powers. To sketch the secondary legal framework, an encyclopaedia approach is taken, exploring relevant legal rules in both the public and the private domain. Among all the existing areas of law, only those that are *prima facie* relevant for the protection of an individual in

---

[241] This section uses excerpts from the article: Helena Ursic and Bart Custers, 'Legal Barriers and Enablers to Big Data Reuse A Critical Assessment of the Challenges for the EU Law' [2016] European Data Protection Law Review 1.

[242] These were the European Coal and Steel Community Treaty in 1952 (now expired), and the European Economic Community Treaty and the Atomic Energy Community Treaty in 1957. Gráinne de Búrca, 'The Road Not Taken: The EU as a Global Human Rights Actor' (2011) 105 American Journal of International Law 649, fn 5.

[243] According to Article 6 of the TEU the body of EU human rights law consists of three main sources: the EU Charter of Fundamental rights, the European Convention of Human Rights and member states' constitutional traditions. The Court of Justice of the EU (CJEU) had referred to these sources decades before the TEU was adopted. It had articulated and developed them through the doctrine of general principles of EU law, which is a set of legal principles, including human rights, that represents a catalogue of most basic concepts and aspirations of EU law. Paul Craig and Grainne De Burca, *EU Law: Text, Cases, and Materials* (Sixth Edition, Oxford University Press 2015) 380. This does not mean, of course, that human rights were less relevant to the EU law before the adoption of the Charter. In fact, De Burca argues that the human rights mechanism as envisioned by the EU founding fathers was even more robust than the one we have today. Búrca (2011) 3.

[244] See for example Case 36/75, *Rolan Rutili v. Minister for the Interior* [1975] 1975 E.C.R. 1219, 32.

the data economy are considered. This selection of relevant legal areas is thus limited to four domains: data protection (including ePrivacy), cyber security, competition, and consumer protection.

Throughout the study, the main point of interest remains an individual and the protection of his personal data in the data economy. The focus is on *commercial* use and reuse of personal data. However, commercial data processing is oftentimes strongly intertwined with the state intervention on data markets. The state plays several roles on this market: it sets the rules, monitors actors' behaviour, and uses data for its own purposes. A typical example of data use is data processing for the purposes of national safety. For example, the state might collaborate with commercial actors, urging them to share the data that is generated or collocated in the course of their commercial activities.[245] This phenomenon, which Schneier calls a 'public-private partnership on data surveillance', raises some important concerns, most apparently in relation to citizens' privacy.[246] In spite of its relevance for the data economy, however, the analysis of the role of the government falls outside the scope of this thesis and will not be further addressed.

3.2. EU fundamental rights and personal data in the data-driven economy

3.2.1. Introduction

Section 3.2. considers eight fundamental rights and freedoms from the EU Charter.[247] The selection is based on the relevance of the provisions for the protection of an individual and her data. Chapters V and VI of the Charter are excluded since they only address the relations between citizens and the state, which are not in the scope of this thesis. Of the rights listed in Chapter I, only human dignity has been selected, as it represents a concept in which all other rights are grounded. Other provisions in this chapter are too closely attached to the protection of human body to be considered. Furthermore, four provisions have been selected from Chapter II 'Freedoms': Article 7 protecting private and family life, Article 8 protecting personal data, Article 11 granting freedom of expression, and Article 16 recognising freedom of business. Although the latter does not refer to individuals, it might be an important guideline to balance interests in relation to commercial data processing. Chapter III comprises several provisions that all prevent discrimination and safeguard equality. For the purposes of this analysis, the chapter is considered as a whole, i.e. general prohibition of discrimination. Chapter VI's provisions that regulate the employer-employee relations are disregarded as are provisions on the protection of health, environment, and social security. However, Article 38 on consumer protection proves relevant for data subjects' position in the economy, as data subjects are typically consumers.[248]

The sequence in which the rights and freedoms are listed in this section reflects their relevance for the protection of an individual and her data. The right to private and family life is placed first, followed by

---

[245] Facebook's transparency report reveals that between January and June 2017 the company received 32.716 requests for information by different US state authorities: <https://transparency.facebook.com/country/United%20States/2017-H1/> accessed 30 May 2018. In the same period, Twitter received more than 2000 requests: <https://transparency.twitter.com/en/information-requests.html> accessed 30 May 2018. The US authorities are not the only ones making use of the private actor data. As Facebook's and Twitter's websites demonstrate, virtually every state collaborates with the large data holders.

[246] See more in Schneier (2015) Chapter 6.

[247] All the bellow mentioned rights are subject to limitations of the Charter's scope and reach. The Charter cannot extend EU's competences and can be only applied by the national authorities when they are implementing EU law (Article 51 of the EU Charter).

[248] Rhoen, 'Beyond Consent: Improving Data Protection through Consumer Protection Law' 1.

the right to personal data protection. These two rights are explored in detail, as they are directly relevant for data processing in the data-driven economy. Since the right to private life directly corresponds to Article 8 of the ECHR, a short analysis of the relevant ECHR provision and the European Court of Human Rights' case law is provided too. Subsequently, the focus shifts to other rights which play significant albeit indirect roles in protecting individual data: prohibition of discrimination, protection of consumer rights, and the freedom of expression and information. Finally, human dignity and the rule of law are discussed as two underlying principles in the system of fundamental rights protection. Freedom to do business does not refer to individuals *per se* but it is an important consideration for the balancing between individual and commercial interests in personal data. Accordingly, this provision is briefly described at the end of the individual rights overview.

Human rights are traditionally characterised by the principles of inalienability,[249] universality,[250] indivisibility, interdependency,[251] and interrelatedness.[252,253] These characteristics point to their fundamental character and guidance role in all sorts of interactions. Charles R. Beitz defines fundamental rights or human rights[254] as '*the constitutive norms of a global practice whose aim is to protect individuals against threats to their most important interests arising from the acts and omissions of their governments (including failure to regulate the conduct of other agents)'.*[255] The fact that the conduct of non-governmental agents, including commercial entities, is part of the core definition of human rights, is of utmost importance for this thesis, which focuses on the relation between individuals and commercial data users.

However, the degree to which the Charter could help defend individual rights before courts, or in other words, the extent to which individuals could invoke their rights on the basis of the Charter, is disputable. As Article 52 stipulates, the Charter's provisions have to be respected by all EU institutions and by EU member states when they implement EU law. This means that the Charter will primarily impact the states, and *not* private parties. All policies and legal actions taken by the European institutions and transposing national laws have to pay attention to the Charter's provisions. Nevertheless, the Charter might also have effects on private parties in the sense that it can extend to

---

[249] See for example EU Charter, Article 52 (1). Inalienability means that human rights are inherent to all human beings and cannot be lost. Their suspension or a restriction must be set by the law.

[250] As for universality, human rights apply equally to all people everywhere in the world, and with no time limit. Universality is a contentious concept as it might apply that rights should be synchronically universal. Raz stresses the difficulty of universality and its sensitivity to cultural variations. For the EU human rights law the issue of universality is somewhat resolved since what the Charter requires is universality across the EU. Joseph Raz, 'Human Rights in the New World Order' (2009) 47 <https://core.ac.uk/download/pdf/13553265.pdf> accessed 29 May 2018.

[251] The concept of interdependence and indivisibility contends that these rights are mutually reinforcing and equally important. Helen Quane, 'A Further Dimension to the Interdependence and Indivisibility of Human Rights: Recent Developments Concerning the Rights of Indigenous Peoples' (2012) 25 Harvard Human Rights Journal 55, 50.

[252] Vienna Declaration and Programme of Action Adopted by the World Conference on Human Rights in Vienna on 25 June 1993 (I (5)), Universal Declaration of Human Rights (Preamble) <http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx> accessed 19 August 2018.

[253] Furthermore, human rights are indivisible, interdependent and interrelated. They are intrinsically connected and cannot be viewed in isolation from each other <http://www.coe.int/en/web/compass/what-are-human-rights-> accessed 29 May 2018.

[254] According to the European Union Agency for Fundamental Rights (FRA), the term 'fundamental rights' is used in a constitutional setting whereas the term 'human rights' is used in international law. The two terms refer to similar substance as can be seen when comparing the content in the Charter of Fundamental Rights of the European Union with that of the European Convention on Human Rights and the European Social Charter. In this thesis, I will use the terms interchangeably. <http://fra.europa.eu/en/about-fundamental-rights/frequently-asked-questions> accessed 29 May 2018.

[255] Charles R Beitz, *The Idea of Human Rights* (Oxford University Press 2009) 197.

horizontal relationships. The possibility of its direct horizontal effect was confirmed in *Kücükdeveci*.[256] As for the indirect effect, the Charter has a strong imperative force and can be used for the interpretation of private obligations and state measures which affect private relations.[257] Furthermore, the Courts are bound to safeguard fundamental rights and may enforce them in disputes between private parties too. Finally, the Charter has the possibility of a direct horizontal effect in relation to the provisions that address private parties or in which the rights are sufficiently concretised.[258]

The feasibility of the Charter's effect has already been communicated to the data economy by the CJEU. In the landmark decision in *Google Spain,* the Court proved that private actors could be strongly influenced by the provisions of the Charter.[259] Following the judgement, Google had to establish a complex (and costly) process to handle thousands of data removal requests.[260] This sent an important message to the markets. As long as the data economy actors operate with fundamentally protected artefacts, they cannot disregard the EU Charter's provisions.

As a final remark, some authors have warned of current proliferation of human rights in terms of inflation.[261] This thesis likewise takes the stance that new rights are not needed, but rather the traditional ones need to be interpreted in a new light.[262] However, enhancing fundamental rights in a digital environment proves challenging. The traditional vocabulary on rights lacks the tools to analyse all the specificities of the Internet space in light of fundamental human interests and needs.[263] Meagre jurisprudence is an additional hurdle. This section is an attempt to translate traditional principles into the data economy language.

---

[256] C-555/07, *Kücükdeveci* [2010] ECLI:EU:C:2010:21.
[257] Takis Tridimas, 'Fundamental Rights, General Principles of EU Law, and the Charter' (2014) 16 Cambridge Yearbook of European Legal Studies 361, 390.
[258] Ibid.
[259] C-131/12, *Google Spain* [2014] ECLI:EU:C:2014:317.
[260] *Obiter dictum*, many of those tools are not available to individuals who therefore lack direct and easily accessible ways of challenging Member States behaviour before EU courts. Collective litigation or individual redress before the ECHR could mitigate the gap. Laura Ferrara, 'Working Document on Establishment of an EU Mechanism on Democracy, the Rule of Law and Fundamental Rights - Litigation by Citizens as a Tool for Private Enforcement' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-575.319+01+DOC+PDF+V0//EN&language=EN> accessed 30 May 2018.
[261] See a summary of their ideas in Urbano Reviglio, 'A Right to Internet Serendipity? An Alternative Way to Tackle the Threats of an over-Personalized Internet Experience' The 2016 Internet, Policy & Politics Conference, Oxford Internet Institute, University of Oxford (2016) <http://ipp.oii.ox.ac.uk/sites/ipp/files/documents/Internet%2520Serendipity.Reviglio.Oxford.pdf> accessed 19 August 2018.
[262] See for example Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009). I limit my remark to the fundamental rights discussion, whereas secondary law could, in my opinion, benefit from certain changes in the framework.
[263] Reviglio (2016).

3.2.2. Protection of private life in the EU system of fundamental rights

3.2.2.1. The ECHR system of protection of personal data and private life

3.2.2.1.1. The right to private life under Article 8 of the ECHR

The fundamental need for private life (privacy) is inherent to a human being[264] and extends to many areas of one's life. However, there is no universally accepted definition of privacy. Legislatures, judiciaries, and scholars have understood and described it in multiple ways.

In the late 19th century, legal scholars Warren and Brandeis first defined privacy as the right to be let alone. With the introduction of the tort of 'invasion of privacy' they intended to mitigate problems that emerged as a result of new technologies such as cameras.[265] Later it became clear that privacy is a concept broader than Warren and Brandeis' first conceptualisation. The subsequent academic and judicial discussion highlighted several principles, all deeply entrenched in the idea of privacy.[266] Since the early 20th century the understanding of privacy has been dependant on technological developments and their impact on society. In the light of new information technologies, a particular point of attention became informational privacy, a concept closely related to the idea of control over someone's data. Alan Westin's call for more attention to privacy's informational aspect was especially insightful: *'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to.'*[267] Today, a vast number of activities in the private or public sector are connected, in one way or another, with the collection and processing of personal information. Therefore, informational privacy in the modern world should be understood not as a separate form of privacy but as an overarching concept for all other privacy aspects.[268]

When a privacy claim is recognised in a law or in a social convention, such as a constitution or an international agreement, we speak of privacy rights.[269] After the Second World War, the concept of a right to privacy emerged in international law, in Article 12 of the Universal Declaration of Human Rights, according to which no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence.[270] The European legal tradition firmly regarded privacy as a fundamental right.[271] The right to privacy was explicated in Article 8 of the ECHR, which protected 'private and family life' and 'home and correspondence'.

---

[264] This inherent and universal idea of privacy is well-explained in Alan F. Westin, *Privacy and Freedom* (Ig Publishing 2015).
[265] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[266] See for example Solove, 'Conceptualizing Privacy'.
[267] Westin (2015) 5.
[268] See Bert-Jaap Koops and others, 'A Typology of Privacy' (2016) 38 University of Pennsylvania Journal of International Law.
[269] Alan F. Westin, 'Social and Political Dimensions of Privacy' (2003) 59 Journal of Social Issues 431.
[270] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' <https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf> accessed 29 May 2018.
[271] The variety of doctrinal descriptions through which privacy is enshrined explains the importance of privacy for European regulators but also unalignment of national constitutions when it comes to privacy protection. Based on a thorough analysis of national constitutions, a research group from Tilburg University identified 13 groups of objects which closely related to citizens' private sphere and were afforded constitutional protection, among others, personal data, thoughts, social relations, family, places and mediated communications. These objects are reflections of various values that need to be constitutionally protected by the right to privacy. Koops and others (2016).

Article 8 of the ECHR is far from being a narrow notion, and the European Court of Human Rights (ECtHR) has interpreted it generously, taking into account many of the abovementioned privacy aspects. Through the ECtHR case law, the Article 8 right has shown different facets: from privacy as solitude, opacity, or seclusion,[272] privacy as non-interference and liberty,[273] privacy as autonomy,[274] and finally, privacy as informational control.[275] Such an open interpretation is important for the protection of privacy in the digitalised and datafied world, as it means that the court (ECtHR) has the means and the willingness to incorporate values in new environments dominated by modern technologies.[276]

In the big data environment, asserting privacy breaches is challenging. Typically, such breaches are hypothetical, future, and non-individual (*in abstracto* harm), which the ECtHR, in principle, does not take into consideration. In some limited cases, the ECtHR has been willing to make an exception and accepted *in abstracto* claims.[277] It is expected that the CJEU will follow the ECtHR's lead.[278] This is an encouraging trend, as in the data-driven economy risks are often non-tangible and highly abstract.[279]

The facet of the right to privacy that refers to personal data is sometimes described as 'informational privacy' and to a great extent corresponds to the right to data protection under the EU Charter. The section below describes how the ECtHR interprets personal data protection within the broader framework of Article 8.

3.2.2.1.2. Protection of personal data under Article 8 of the ECHR

In relation to privacy of personal information, the ECtHR holds that the core principles of data protection which the Court extracted from the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981 (Convention 108)[280] require the retention of data to be proportionate in relation to purpose of collection and envisage limited periods of storage.[281] Furthermore, disclosure of individual data to third parties may result in a violation of the ECHR.[282] For example, wide accessibility of personal data, in particular sensitive data,

---

[272] For an overview of the Court's jurisprudence see Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the criminal law* (Intesentia 2006).

[273] In the sense of the landmark US Supreme Court's decision in *Roe v. Wade* (410 U.S. 113 (1973)) on abortion rights; also see: Koops and others (2016).

[274] Pretty v. United Kingdom, 2346/02 [2002] ECHR 423 (29 April 2002) – using the Article 8 right to justify the right to die with assistance. Also see Council of Europe/European Court of Human Rights's Guide on Article 8 of the European Convention of Human Rights, updated on 31 August 2018 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 27 December 2018.

[275] The part of Article 8 of the ECHR that ties to the idea of data protection. See for instance Peter Hustinx, 'European Leadership in Privacy and Data Protection' 1 <https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf> accessed 29 May 2018.

[276] Barbulescu v Romania - 61496/08 [2016] ECHR 61 (12 January 2016) concerning the use of the internet in the office.

[277] Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities BT - Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds) (Springer Netherlands 2016) 415.

[278] See for example the judgement of 8 April 2014, *Digital Rights Ireland*, C-293/12, ECLI:EU:C:2014:238.

[279] Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information & Communications Technology Law 74, 1.

[280] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (open for signature on 28 January 1981, entered into force on 1 October 1985).

[281] S and Marper v United Kingdom, 30562/04 [2008] ECHR 1581 (4 December 2008), para. 41.

[282] Surikov v Ukraine, 42788/06 [2017] ECHR 100 (26 January 2017), para. 86.

can undermine the protection of family and private life. A simple press release, for example, issued in an individual case with no intention for it to be posted on the Internet, may well be picked up by third parties and discussed on the web to the detriment of the individual's right to private and family life.[283] As explained above, the convention provides no direct redress to private parties. However, states might be liable for allowing third parties to store data on individuals.[284] When this is the case, there should be no obstacle for an individual to assert her rights under the ECHR.

When defining personal data, the ECtHR traditionally follows the OECD guidelines.[285] The OECD describes personal data as any information that directly or indirectly relates to an individual.[286] However, in the case of *Magyar Helsinki Bizottsag v. Hungary*, the Court departed from this conventional approach and adopted a narrower definition of personal data in the public domain.[287] In a dissenting opinion, judges Nussberger and Keller opposed the argument that data that is already in the public domain and has been published needs less protection. Protection of personal information has one important determinant – a person's informational self-determination – which should be guaranteed regardless of whether the data is in the public domain or remains confidential.[288] In their view, the notion of 'private life' in Article 8 should as a rule continue to protect both published and unpublished personal data. While determining the boundaries of Article 8 in relation to personal data, the two judges also drew on the recent CJEU jurisprudence in relation to the EU's unique right to data protection.[289] This dissenting opinion is an important recognition that in the era of data proliferation, data no longer needs to be restricted to a private space and access to guarantee privacy protection. In the following chapters, it is shown that even if a person wants to keep the data for himself, this is becoming increasingly difficult. Therefore, it is critical that the Court acknowledges the need to also protect data that has leaked into a public space.

3.2.2.2. Privacy and data protection as part of the EU framework of fundamental rights

Before the adoption of the Charter, the CJEU adjudicated upon privacy and data protection related cases in light of the ECtHR jurisprudence.[290] However, the Treaty on the Functioning of the EU (TFEU) gave a binding nature to the Charter of the Fundamental Rights of the European Union (Charter),[291] which set out the right to data protection in its Article 8, in addition to the right to privacy in Article 7. Thus, since 2009, the CJEU can refer directly (and exclusively) to the provisions of the Charter.

The TFEU not only gave a binding nature to the Charter, it also recognized data protection as a fundamental right and introduced an explicit basis for the enactment of data protection legislation (Article 16). Restating the fundamental nature of data protection and urging the EU legislator to adopt

---

[283] Council of Europe/The European Court of Human Rights: Research Division, 'Internet: Case Law of the European Court of Human Rights' (2015) 16 <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 14 June 2018.
[284] Drawing on P. and S. v. Poland, 57375/08 [2008] ECHR (30 October 2012).
[285] The first version of the OECD privacy guidelines was published in 1980. In 2013 the guidelines were revised. The current version is available at: https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm.
[286] Ibid.
[287] Magyar Helsinki Bizottsag v. Hungary, [2016] 18030/11 ECHR (8 November 2016).
[288] Para. 8 of the dissenting opinion of judge Spano joined by judge Kjølbro in Magyar Helsinki Bizottsag v. Hungary, [2016] 18030/11 ECHR (8 November 2016).
[289] Ibid., para. 9.
[290] See for example C-468/10 *ASNEF* [2011] ECLI:EU:C:2011:777; C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662.
[291] 2000/C 364/01 [2000] OJ C 364/3

implementing legislation was a significant improvement, [292] indicating the great importance of data protection for the EU. Section 3.2.2.2.2. further explains the implications of this amendment.

3.2.2.2.1. The right to private life and protection of privacy of personal data under Article 7 of the EU Charter

Article 7 guarantees *'the right to respect for his or her private and family life, home and communications to everyone.'* Since the provision is almost identical to Article 8 of the ECHR, the ECtHR case law has remained an important source.[293]

The CJEU has interpreted the right in Article 7 broadly, encompassing the physical, psychological, and moral aspects of the personal integrity, identity, and autonomy of individuals.[294] For example, the right to privacy under Article 7 has been used to grant protection from intrusive home searches, guarantee confidentiality of communications, and even ensure environmental protection. As is the case with Article 8 of the ECHR, Article 7 of the Charter has also been used to safeguard privacy of personal data. In the *ASNEF* case, the CJEU argued that compromising non-public data was a '*more serious infringement of the data subject's rights […]'* under both Articles 7 and 8 of the Charter.[295]

As the previous section explained, the Charter introduced a new right to data protection, which is explicated in Article 8. This article is closely related to Article 7, as protection of personal data and protection of someone's personality are interconnected. This close relationship is the reason why introducing Article 8 in the Charter did not cause any major changes in the CJEU argumentation of informational privacy. Most often, the Court simply conflates the two rights.[296]

The question therefore arises of why the new right was implemented if Articles 8 and 7 are almost always interpreted as a whole. Why is Article 7 an insufficient guarantee of personal data protection? The following section aims to identify reasons for the new right to data protection and explores how it could be disentangled from the right to privacy.

3.2.2.2.2. The right to data protection in Article 8 of the EU Charter

The EU Charter defines the right to data protection in Article 8. The provision starts with a general guarantee of protection of personal data to everyone whom the data concerns. The next paragraph stipulates that *'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.* The Charter also provides for *'access to data which has been collected concerning him or her, and the right to have it rectified.'* Finally, an independent authority should control compliance with the data protection rules.

The data economy perceives personal data as an economic resource rather than an extension of individual personality. The right to data protection therefore comes as a counterbalance to this overly economic approach to personal data and indicates the potential for protection of individuals in the

---

[292] Hielke Hijmans, 'The European Union as a Constitutional Guardian of Internet Privacy and Data Protection' (University of Amsterdam 2016), in particular Chapter 4.
[293] C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others* [2003] EU:C:2003:294, para 73. Also see EU Charter, Article 52.
[294] Steve Peers and others, *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014) 156.
[295] C-468/10 *ASNEF* [2011] ECLI:EU:C:2011:777, para. 45.
[296] Lynskey (2015) 90. See also Judgement of 9 November 2010, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*, C-93/09, E.C.R. [2010] I-11063.

data-driven economy. However, the new right has also led to some daunting questions. First, the reasons for its codification in the Charter (and in the TFEU), which could be a useful guideline in delineating the scope of the right, are not entirely clear. Second, the relationship with Article 7 is disputable and the line between the two rights is blurred. The recent CJEU case law has not been particularly helpful in disentangling the two rights. In fact, its interpretation has raised more questions than it has provided answers. These uncertainties suggest that we have yet to see what Article 8 actually means for the protection of individuals in the data-driven economy. To anticipate what the right could bring for the future protection of individuals, two questions are explored: 1) what justifies the introduction of personal data protection as a human right, and 2) how it differs from the long-established right to privacy.

3.2.2.2.2.1. The reasons to codify data protection as a human right

To answer the first question, we need to examine recent history. The first considerations on a data protection right substantially preceded the Charter. In light of new technological developments in the early 1970s, the Council of Europe concluded that Article 8 of the ECHR suffered from a number of limitations.[297] This was one of the first moments when the idea of a stand-alone right to personal data protection was publicly expressed.

In the subsequent years, three important rationales gave rise to the creation of the new right. First, the data protection regime in the EU needed additional legitimacy. In the 1990s, the EU already adopted secondary legislation that protected personal data when flowing across the internal market. This data protection regime, which was based on the data protection directive, had a binary nature. On the one hand, its objective was to support the free flow of information. On the other hand, it also entailed the 'rights objective', which aimed to safeguard personal data and privacy. While the free flow objective perfectly suited the single market goal of the EU treaties, the 'rights objective' somehow lacked a foundation in these treaties. There was a danger that without a normative anchor, the EU data protection system, rooted in the values of informational self-determination and autonomy, would be reduced to a mere set of administrative rules channelling the flow of personal data.[298]

Second, the new right to data protection was necessary to embrace the changes in society as a result of new, digital technologies and to incorporate them in the fundamental instruments. In Code 2.0, Lessig writes about a transformative nature of the constitution: '*A transformative constitution (or amendment) […] tries to change something essential in the constitutional or legal culture in which it is enacted—to make life different in the future, to remake some part of the culture.*'[299] De Hert and Gutwirth assign such a transformative nature to the EU Charter through the new provisions on data protection and human dignity.[300]

---

[297] Francesca Bosco and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (2015) 5.
[298] Lynskey (2015) 255.
[299] Lessig (2006) 313.
[300] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 11-12.

This second rationale of data protection has been confirmed by the substantial increase in litigation on data protection before the CJEU.[301] Between 1970 and 2009, there were 24 cases on data protection matters. Between 1 December 2009 and 2016, the number has increased substantially, with the Court having received over 120 cases (including pending).[302] The Court has dealt with the questions of how data should be protected on the Internet,[303] how online data protection and privacy should be balanced with other fundamental rights such as (intellectual) property,[304] what sort of information should the right protect in light of developing technologies,[305] and who should be held responsible for guaranteeing privacy.[306] It can indeed be argued that by introducing the new right in its jurisprudence, the CJEU fully embraced the idea of evolving interpretation in the sense of Lessig's 'technology constitution'.

Finally, data protection does not solely serve privacy, but also supports some other objectives. One such objective is self-determination, as shown by the infamous German Census case[307] and as quoted in the recent ECtHR dissenting opinion.[308] Likewise, the CJEU has already admitted that data protection could safeguard some other values in addition to privacy.[309] These values that go beyond privacy could explain why data protection objectives cannot be simply subsumed under Article 7 of the Charter. Below these differences are elaborated in more detail.

3.2.2.2.2.2. Differences between the data protection right and the right to privacy

The right to data protection and the right to private life are closely related, but they are not interchangeable. In many aspects, the right to data protection is narrower in scope than the right to data privacy. Data privacy clearly applies in situations where data protection does not, for instance in cases of physical privacy interferences[310] or when data is anonymised.[311] However, data protection may

---

[301] Tridimas (2014) 363.

[302] The research was conducted through the CJEU case-law database "Curia" on November 15, 2016, http://curia.europa.eu/juris/recherche.jsf?language=en.

[303] C-101/01, *Lindqvist* [2003] ECLI:EU:C:2003:596.

[304] C-275/06, *Promusicae* [2008] ECLI:EU:C:2008:54.

[305] C-582/14, *Breyer* [2016] ECLI:EU:C:2016:779.

[306] C-131/12, *Google Spain* [2014] ECLI:EU:C:2014:317. 'In *Google Spain* the Court took into consideration the changed reality in the information society, which has an impact on privacy and data protection and on the balancing between fundamental rights. The ubiquitous availability of information implies a lack of control on the part of the data subjects and potentially restricts their autonomy.' Hielke Hijmans, 'The European Union as a Constitutional Guardian of Internet Privacy and Data Protection' (University of Amsterdam 2016) 257. The Court's unanticipated approach imposed a social responsibility on search machines, requesting them to balance between fundamental rights. By assigning them with a task close to the duties of government, the Court no longer differentiated between private and public entities and made a transformative constitutional step.

[307] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07.

[308] Magyar Helsinki Bizottsag v. Hungary, Application no. 18030/11, judgement from 8 November 2016, Concurring Opinion of Judges Nussberger and Keller, para. 7.

[309] In *Rynes* the CJEU held that *'Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter […] the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed.'* It is evident from this diction that data protection also aims at protecting other values and freedoms besides privacy.

[310] Lynskey (2015) 11.

[311] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' 5 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 27 December 2018.

sometimes be wider than (informational) privacy.[312] This is the case when personal data has been deliberately made public, meaning that the right to privacy has been waived and consequently Article 7's protection should no longer be granted. In such circumstances, however, data protection remains applicable and therefore offers broader protection.[313] The ECtHR's judges in *Magyar Helsinki Bizottsag v. Hungary* noted the same point by acknowledging that protection of personal information, which is closely related to the concept of informational self-determination, should be guaranteed regardless of whether the data is in the public domain or remains confidential.[314] In the US, publicly disclosed data falls outside of the expected privacy protection of the Fourth Amendment.[315] In the *Jones* case, the US Supreme Court Justice Sotomayer challenged this doctrine: '*More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. […] This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.'*[316] In the EU, such cases may to some degree be mitigated with the data protection rules.[317]

Beyond the difference in scope, data protection and privacy should be distinguished because of different underlying objectives. Lynskey indicates two of them: 1) the development of individual personality and 2) reducing the power and information asymmetries between individuals and those who process their data.[318] Regarding the first, an illustrative example is the German Federal Constitutional Court's decision on census law. In this landmark judgement, the Court drew on the concept of self-determination to tackle the dilemma of collection and processing of personal data on a large scale.[319] Building on the concept of human dignity, the Court established the right to informational self-determination. In the Court's view, any processing of personal data should in principle be regarded as an interference with the right to informational self-determination, unless the data subject has consented to it.[320] In other words, the right to self-determination requires that everyone should in principle be able to determine for herself the disclosure or use of her own personal

---

[312] Case T-194/04, *Bavarian Lager v. Commission* [2007] ECR II4523, para. 67. '*According to the EDPS, the interest protected […] is private life and not the protection of personal data, which is a much broader concept. Whilst the name of a participant, mentioned in the minutes of a meeting, falls within the scope of personal data, since the identity of that person would be revealed and the concept of the protection of personal data applies to those data, whether or not they fall within the scope of private life, the EDPS points out that, in the area of professional activities, the disclosure of a name does not normally have any link to private life. […].'*

[313] Lynskey (2015) 11.

[314] Magyar Helsinki Bizottsag v. Hungary, Application no. 18030/11, judgement from 8 November 2016, Concurring Opinion of Judges Nussberger and Keller, para. 7.

[315] Brief for the competitive Enterprise Institute, Cato Institute, Reason Foundation, and Committee for Justice as amici curiae in support of petitioner Timothy Ivory Carpenter, 11 August 2017, p. 15 <https://object.cato.org/sites/cato.org/files/wp-content/uploads/carpenter_merits.pdf> accessed 27 December 2018.

[316] United States v. Jones, 132 S.Ct. 945 (2012).

[317] E.g. data minimization, purpose limitation that apply generally to all personal data collected in the course of commercial activities.

[318] Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right To Data Protection in the Eu Legal Order' (2014) 63 International and Comparative Law Quarterly 569, 589 and the following.

[319] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07.

[320] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' 8.

information.[321] The Court did not base the arguments on the provision on privacy[322] but on the first article of the German Basic Law (the German Constitution), focused on protecting human dignity. Indeed, informational self-determination is highly disparate from the idea of privacy as a 'right to be let alone'. It is not concerned with the absence of external factors but with active presence of data. As such, it better corresponds to the right to data protection.[323] In fact, the right to self-determination has been described as a cornerstone of the maturing right to data protection.[324]

As the second example of how privacy and data protection serve different goals, Lynskey cites the English case of *R v Brown*.[325] In this case, a police officer accessed the Police National Computer (PNC) database on two occasions to assist a friend who ran a debt-collection agency by checking vehicles owned by debtors from whom the agency had been employed to recover debts. No personal data was retrieved on the first occasion; on the second occasion, personal data was revealed but no subsequent use was made of that data. On appeal, the House of Lords held that something had to be done with the data beyond accessing it for criminal sanctions to ensue. Lynskey points out that if a purposive (teleological) approach to data protection had been taken in this context, it could have been argued that the access to the personal data on the PNC database for entirely unauthorised purposes exacerbated the power asymmetries between the police officers – the data controllers – and the individual, and therefore the data protection rules should apply, even though privacy of the records was not violated.

On a more practical note, Kranenborg sees the specifics of the right to data protection in its unique mission, that is addressing technological developments and the increasing use of information (communication) technologies.[326] The right sets up a unique system of check and balances, particularly needed in the modern data processing reality. Similarly, Gellert describes data protection as a means to tame the effects of this technology on society, and to address the risks to privacy and other fundamental rights.[327] In his view, the right to data protection resembles risk-oriented regulations such as environmental law.

Both Geller's and Kranenborg's views are interesting and important for this thesis. First, they recognise the added value of data protection within the system of human rights. Second, they acknowledge that the right is gaining increasing prominence in the data-driven economy.[328]

---

321 <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf> accessed 29 May 2018.

322 Art. 10 (Privacy of correspondence, posts and telecommunications).

323 Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law and Security Review 84, 86.

324 Yvonne McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (January-June 2017) Big Data & Society 2.

325 House of Lords' judgment in *R v Brown* (Gregory Michael) [1996] AC 543.

326 Herke Kranenborg, 'Article 8', in Peers and others (eds) *The EU Charter of Fundamental Rights. A Commentary* (Hart Publishing 2014) 264.

327 Raphael Gellert, 'Understanding Data Protection as Risk Regulation' (2015) 18 Journal of Internet Law 3.

328 The views on data protection distinct underlining values and on its unique system of check and balances, are brought together in Gutwirth & De Hert's critics of AG's proportionality discussion in the opinion in the *PNR case.* By using privacy as the only counter measure to the proposed collection of passengers' data, AG allegedly missed the potential of data protection to address the issue. *'Rather than a limited formal compliance check from our judges, we expect a strict review of all the different alternatives encountered and their different impact on privacy and individual rights. Does the US need 34*

In spite of the attempts in theory and practice to separate and justify the distinction between the rights to privacy and data protection, they are trapped in a tight relationship. This has been aggravated by the fact that on many occasions, the CJEU has simply conflated the two rights.[329] Hijmans contends that considering the two rights as a whole is in fact the solution to the dilemma of de-conceptualising privacy and data protection: *'… as a result of the features of the internet and developments of communications on the internet – with big data and mass surveillance as obvious examples – all processing of personal data has a potentially adverse effect on the right to privacy under Article 7 Charter, if only because one cannot know in advance the purposes for which personal information that is available in electronic databases that will subsequently be used.*'[330] If we take Hijmans' view further, the rights in articles 7 and 8 should be considered as one whole, with Article 8 as the instrumental part of the broader right to privacy.

I do not fully agree with Hijmans' 'equalising' approach alyhough I understand his concern for the implications of big data. As explained above, data protection has some unique objectives (e.g., power symetry) that can be easily overlooked if simply merged with the privacy objectives. Moreover, taking the right to data protection as a separate concept is highly relevant for the data economy, from a normative and from an instrumental perspective. From the normative perspective, it puts a strong obligation on everyone to consider protection of personal data. This does not mean that data protection would not be observed if there was no specific provision in the law. In the past, the CJEU was able to develop new rights from some very plain constitutional principles. This could easily happen with data protection, as it is a concept strongly attached to privacy.[331] However, explicit provisions in the TFEU (Article 16) and in the Charter (Article 8) leave no doubt and force the CJEU and other EU institution to consider data protection more carefully. From an instrumental perspective, the data protection provisions give rise to more specific legal measures, which constitute a framework for those who handle personal data daily to do this in a caring and legitimate way. In addition, it emphasises the importance of instruments that enhance the active role of individuals in determining their personal data uses.

3.2.3. The prohibition of discrimination

Chapter III of the EU Charter is dedicated to equality. Article 20 stipulates that '[e]veryone is equal before the law.' Article 21 prohibits discrimination 'based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion,

categories of data? Why are the EU PNR agreements concluded with Australia and Canada less infringing on human rights? Are Australian and Canadian security forces wrongly less demanding or do they combine security and privacy better?' In Gutwirth & De Hert's view AG Leger should have used the right to personal data protection (and its unique check and balances' system) to highlight the protection of values that are not necessarily the same as those protected directly by the right to privacy (e.g. transparency of algorithms and monitoring). De Hert and Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' 38.

[329] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 271. Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law.

[330] Hijmans (2016) 54.

[331] See the discussion above in section 3.2.2.2.2.

membership of a national minority, property, birth, disability, age or sexual orientation'. The second paragraph of Article 20, prohibiting nationality-based discrimination, is EU-specific.[332,333]

By nature, provisions on fundamental rights are open-ended and require interpretation. The CJEU has had a dominant role in interpreting the provisions related to the issues of equality and discrimination. As a reflection of the Aristotelian principle, the CJEU defines direct discrimination as occurring when one person is treated less favourably than another person on one of the protected grounds.[334] In contrast, indirect discrimination is encountered where some requirement is demanded, some practice is applied, or some other action is taken that produces an 'adverse impact' for a protected class of persons.[335] The requirement or the practice itself may not be prohibited but the consequence of the conduct is differentiation between persons on prohibited grounds.

In limited cases, the Court allows discriminatory conduct. However, such unequal treatment must be based on objective considerations, independent of the nationality of the persons concerned, and must be proportionate to the objective being legitimately pursued.[336] Besides, positive discrimination may be legitimate when it gives advantage to those groups in society that are often treated unfairly because of their race, sex, etc.[337]

The intensive use of data in the modern data economy increases the risk of discrimination, in particular indirect discrimination. As indicated in Chapter 2, big data and its reuse may be highly useful for profiling purposes, but the results of profiling and other types of data analyses may be stigmatising or discriminatory. Algorithms driving big data analytics may find correlations between risk and vulnerable

[332] Besides the EU Charter, discrimination is also prohibited in a number of other international human rights instruments. Amongst them, the Universal Declaration of Human Rights plays a significant role. The source, which the CJEU most often refers to, is the ECHR. Article 18 of the ECHR prohibits discrimination based on a number of personal statutes such as sex, sexual orientation, nationality, religion, disability, age, race, language, political opinion, social origin, property etc. Protocol 12 adds a general prohibition of discrimination. Even though the EU is not yet actually a signatory to the ECHR, the CJEU is largely consistent with the ECHR. However, not all the member states are signatories of the Protocol 12.

[333] Before the adoption of the Charter the EU non-discrimination law was limited to a few directives which addressed the problems of discrimination only partially, to the extent that the discriminatory behaviour related to the common market objectives: Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services and Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (amended). This meant that the scope of anti-discrimination law in the EU was narrower in comparison to the ECHR. European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Non-Discrimination Law* (2011) 57. However, the CJEU ruled that the EU was bound by the general prohibition of discrimination in the ECHR, through the "general principles formula", which included all human rights provisions safeguarded by national constitutions and international documents, including those set in the ECHR. See for example C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others* [2003] EU:C:2003:294.

[334] Philippa Watson and Evelyn Ellis, *EU Anti-Discrimination Law* (Oxford University Press 2012) 143.

[335] Ibid., 142.

[336] C-524/06, *Huber v Federal Republic of Germany* [2008] ECLI:EU:C:2008:724.

[337] European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Non-Discrimination Law*, 35.

classes based on non-causal factors without using personal characteristics that fall under the catalogue of prohibited grounds.[338] This can happen in both the public and private sectors.[339]

Research has shown that removing sensitive attributes (such as ethnicity, gender, etc.) from databases does not necessarily prevent the creation of discriminating profiles.[340] Often, the remaining attributes will still allow for the identification of the discriminated community.[341] For example, gender can be linked to the fact that a person works part time or full time, leading to a classifier with indirect gender discriminatory behaviour based on the type of the employment contract. This would constitute indirect discrimination.[342] Business practices in the insurance sector are particularly illustrative. Property insurers tend to base higher property insurance rates on crime statistics. As people of colour primarily live in areas with higher crime rates, the higher premium calculated according to the rate of crime strongly correlates with race.[343]

Furthermore, it is often taken for granted that big data algorithms produce objective judgements. Contrary to this belief, algorithms often contain hidden biases which may also lead to discriminatory outcomes. For example, a recruitment program may use an algorithm that learns from past hiring patterns. If the patterns are discriminatory, the algorithm internalises them nonetheless. Thus, the discriminatory hiring may continue or even intensify without users even noticing.[344]

The difficulty with imposing liability on the basis of indirect discrimination is a typical obstacle for fighting against discriminatory data-driven practices.[345] Oftentimes, those who employ algorithms are not even aware of discrimination occurring, which raises further questions regarding whom to assign the burden of proof to, what standard of evidence is sufficient to prove the discrimination, and what sort of causality there should be.[346]

---

[338] Rick Swedloff, 'Risk Classification's Big Data (R)evolution' 21 Conecticut Insurance law Journal 339, 360.
[339] Pasqaule writes about a health insurance company which bought data on more than three million people's consumer purchases in order to flag health-related actions, like purchasing plus-sized clothing. Thus, the data on the size of the clothes can be a proxy for their health condition. Pasquale (2015) 233.
[340] Faisal Kamiran and Toon Calders, *Data Preprocessing Techniques for Classification without Discrimination* (2012).
[341] Dino Pedreshi, Salvatore Ruggieri and Franco Turini, 'Discrimination-Aware Data Mining', *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining* (ACM 2008) 29.
[342] Case C-236/09, *Association Belge des Consommateurs Test-Achats ASBL and Others Deutschland* [2010] ECLI:EU:C:2010:564, Opinion of AG Kokott, rec. 69. AG Kokott noted that the use of actuarial factors based on sex is incompatible with the principle of equal treatment for men and women.
[343] The concept of indirect discrimination as it was described above was developed in the EU legal practice. A related US legal doctrine is the so-called disparate impact (or effect). This doctrine contents that policies and practices that have a disproportionately adverse effect on protected classes (minorities, women, etc.) can be declared legally discriminatory without evidence of intentional discrimination. Ronald L. Rubin, 'When "Disparate Impact" Bites Back - Is the Consumer Financial Protection Bureau guilty of the same discrimination it polices in the lending world?' *The Wall Street Journal* (March 9, 2016) <http://www.wsj.com/articles/SB10001424052702303824204579423721516531650> accessed 30 May 2018. Barocas and Selbst explored whether the US legislation was able to address big data discrimination in the employment. The findings showed that this was only possible in limited cases by using the doctrine of disparate effect, for which the required standard of proof is significantly low. Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 California law review 671.
[344] Cathy O'Neil and Gideon Mann, 'Hiring Algorithms Are Not Neutral' [2016] *Harvard Business Review*.
[345] For the US context see: Barocas and Selbst (2016) 697.
[346] Ibid.

3.2.4. Freedom of expression and thoughts

Under Article 11 of the Charter, everyone has the right to freedom of expression, which includes the freedom to hold opinions and to receive impartial information and ideas without interference by public authority and regardless of frontiers.[347]

Freedom of expression is a double-sided right. In addition to providing for a speaker's right, it also creates an audience's right: the right to receive information.[348]

In relation to its first manifestation, one problem highly relevant for the data-driven era is the decreased freedom of expression due to the so-called chilling effect. This phenomenon refers to the fact that people may alter their behaviour when they become aware that they are being monitored. This surveillance can have different expressions: state surveillance, private surveillance, or physical surveillance. It can be performed by different means, e.g. by using cameras or through online monitoring (so-called dataveillance[349]). Sometimes the aim is precisely to make people behave 'better', but a more general effect may be that people behave more modestly and reluctantly overall.[350] This subtle but pressing influence of surveillance on human rights has not gone unnoticed by the CJEU. In Digital Rights Ireland, the Court stated: *'First of all, it is true that it must not be overlooked that the vague feeling of surveillance […] is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information and that an interference with the right guaranteed by Article 11 of the Charter therefore could well also be found to exist.'*

The second manifestation of the right to freedom is the right to receive information (also the right to seek information and/or to search). In light of new technologies and the prevalent role of the Internet, this aspect of Article 11 seems increasingly important.[351] For instance, our searches on the Internet are not equal to other users' searches, but are biased by the characteristics of our online behaviour. Since 2009, the Google search engine has been personalising each user's search results.[352] To perform such a personalisation Google uses its PageRank algorithm, which is able to make guesses about who we are and which sites we may want to see.[353] Such 'filter bubbles' or 'personal echo-chambers' can stifle the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish.[354] Article 11's right could be seen as the ground for the regulation of search engines that would prevent the results from being overly skewed by political or commercial motives. Of course, search engine operators may respond by claiming their expression rights, but it has been

---

[347] This right has been explicated in other international agreements such as UN treaties and Council of Europe's documents on which the EU Charter and the CJEU jurisprudence both draw. See more in Peers and others (2014).
[348] Peers and others (2014) 323.
[349] See Roger Clarke's Dataveillance and Information Privacy Home-Page for the explanation of this word <http://www.rogerclarke.com/DV/#SurvD> accessed 2 June 2018.
[350] Daniel Bachlechner and others, 'WP1 Mapping the Scene: D1.2 Report on the Analysis of Framework Conditions (Deliverable for the EuDEco H2020 Project)' (2015) 33 <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/d1.2_analysisoffframeworkconditions-v1_2015-08-31-1.pdf> accessed 30 May 2018.
[351] Peers and others (2014) 322.
[352] Anikó Hannák and others, 'Measuring Personalization of Web Search' 3 <https://arxiv.org/pdf/1706.05011.pdf> accessed 30 May 2018.
[353] Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin Press 2011).
[354] European Data Protection Supervisor, 'Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology' (2015) 13.

suggested that these would be outweighed by the audience's right not to be misled.[355] Finally, it should be borne in mind that search engines and some other companies that form the digital infrastructure of communication have recently developed elaborate bureaucracies, which are effectively governance structures to regulate online speech and expression.[356] However, their governance system faces some major problems: it is often autocratic, non-transparent, and can be waived whenever necessary or convenient.[357] In 2018, the EU kicked off an initiative on hate speech which requires the platforms to set up a system that allows instant removal and monitoring of hate-speech-like content.[358] Less manoeuvre space for the platforms and more transparency for users are what could alter their private governance to be more aligned with the provision of Article 11.

3.2.5. Consumer protection

Consumer protection law is an inherent part of national and international legal systems. However, only a minority of countries have an expressed provision about consumer protection in their fundamental acts and constitutions. The EU and some of the EU member states are the exception.

Article 38 of the EU Charter entails a highly general provision on consumer protection: *'Union policies shall ensure a high level of consumer protection.'* Compared to the rest of the Charter, the provision is open-ended and can hardly give any direct entitlement to consumers. As the CJEU noted in two of its judgements, the provision is barely programmatic and cannot be directly applicable.

In *Rivero*, which was decided in 1996, the CJEU stated that the scope of Article 129a (now 169 TFEU), entailing an almost identical provision as the Charter's Article 38, was limited. The provision stipulated that the Community had a duty to contribute to achieving a high level of consumer protection and to create Community powers on a consumer protection policy, without laying down any obligation on member states or individuals. The Court interpreted the article as a programming provision, stating that *'Article 129a cannot justify the possibility of clear, precise and unconditional provisions of directives on consumer protection which have not been transposed into Community law within the prescribed period being directly relied on as between individuals.'* Only provisions that are precise and clear can be directly applicable. Article 129a did not fall in this category.

Has the Charter's Article 38 changed the Court's position? One recent interpretation of the article can be found in *Pohotovosť s. r. o. v Miroslav Vašuta*.[359] In this case, the Court considered the degree to which the provision from the Charter relates to the application of Directive 93/13. The Court held that *'since Directive 93/13 does not expressly provide for a right for consumer protection associations to intervene in individual disputes involving consumers, Article 38 of the Charter cannot, by itself, impose an interpretation of that directive which would encompass such a right.'* Hence, the Court followed its *Rivero* line of reasoning. The guarantee of consumer protection in Article 38 thus remains an aspiration provision.

---

[355] Peers and others (2014) 333.
[356] Kate Klonick, 'The New Governors: The People, Rules, And Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598, 1664.
[357] Jack M Balkin, 'Free Speech Is a Triangle' 118 Columbia Law Review 7, 19.
[358] Code of conduct on illegal online hate speech <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31811> accessed 23 May 2018.
[359] C-470/12, *Pohotovosť s. r. o. v Miroslav Vašuta* [2014] ECLI:EU:C:2014:101.

Profiling and targeting strategies deployed by some data-driven companies may amount to significantly impairing a consumer's freedom of choice or conduct. The actual impact depends on the persuasive potential of a personalised message and the extent to which the practice reduces the autonomous decision-making process.[360] Consumer protection law which is rooted in the provision of Article 38 could be used to mitigate negative impacts and help consumers. For example, Helberger suggests that if the data is being used not only to provide the service but also to extract extra commercial value from that data, and this is done without telling the consumer, it violates his rights.[361]

Of course, limited freedom of choice and misusing personal information can also be safeguarded by some other rights. Taking the example of data protection law, consumers may, in many situations, be protected by general EU data protection instruments and specific instruments relating directly to consumers (the right to be informed, to have access to data, to object to automated processes, and to provide administrative and judicial remedies). This is why some anticipate that the case law on Article 38 will develop in connection with other subjective rights, such as the right to anti-discrimination, the right to privacy, and the right to freedom of expression.[362] However, a self-standing provision on consumer protection offers an additional layer of protection, pointing to the specifics of the relationship between a weaker party and a more powerful one.

3.2.6. Human dignity

In the EU Charter, human dignity comes in Article 1 and is defined as '*inviolable'.* Dignity must be respected and protected. However, the Charter does not elaborate on the exact meaning of dignity, so it remains an open concept that has been interpreted by many. The same open definition is found in some other key fundamental rights agreements. While the ECHR only briefly mentions dignity in its preamble, the Universal Declaration of Human Rights refers to it in the very first article.

In the scholarly literature, dignity is described as the right to have rights, or as *'a kind of intrinsic worth that belongs equally to all human beings as such*'.[363] The dignity of the human person is thus not only a fundamental right in itself, but also a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data.[364] A 'rich' definition proposed by Campbell includes values such as solidarity, welfare rights, rights to health and well-being, and the acceptance of duties to the community.[365]

In the CJEU case law, dignity was recognised as an important concept years before the Charter came into force. The Court stemmed it from the national constitutions, notably from the German

---

[360] Helberger gives an example of a consumer who is being targeted with diet products after her smart scale has learned that she has gained a couple of kilos. To assert unfair practice under the directive it would be necessary to better understand how deep the fear of gaining extra weight is (is she obese or bulimic, over-or normal weighted, what is her age, does she have a history of (unsuccessful) dieting, etc.), how perceptive to personalisation strategies, how much the timing of the message plays a role etc. Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' 20 <https://www.ivir.nl/publicaties/download/1747.pdf>.

[361] Ibid., 10.

[362] Monika Jagielska and Mariusz Jagielski, 'Are Consumer Rights Human Rights?' [2012] European consumer protection: theory and practice 336, 351.

[363] Neomi Rao, 'Three Concepts of Dignity in Constitutional Law' (2013) 86 Notre Dame Law Review 183, 197 quoting Alan Gewirth.

[364] European Data Protection Supervisor, 'Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology' 12.

[365] Alastair V Campbell, 'Human Dignity and Commodification in Bioethics' in Dietmar Mieth and others (eds), *The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives* (Cambridge University Press 2014) 536.

constitutional tradition. The CJEU's interpretation of dignity in *Omega* is perhaps one of the best known. In this case, the Court found that a laserdome game which involved 'killing' people was in conflict with the EU fundamental rights and principles, notably human dignity. In the Court's opinion, human dignity may be infringed either by the degrading treatment of an opponent, or by the awakening or strengthening in the player of an attitude denying the fundamental right of each person to be acknowledged and respected.[366]

Big data business models and the entire data-driven economy put pressure on human dignity and related values. Violations of dignity may include objectification, where a person is treated as a tool serving the purposes of someone else.[367] Solove argues that in our information society, people's reputation is increasingly constituted by the data that is disclosed about them.[368] As a result, people are also increasingly judged upon their digital representation (the digital person) rather than as human beings of flesh and blood.[369] Practices like profiling reinforce a tendency to regard persons as mere objects.[370]

3.2.7. The rule of law as the cornerstone of the EU human rights system – the relevance for the data-driven era

Together with human rights protection and democracy, the rule of law represents *'the Union's Holy Trinity.'*[371,372] There is no codified agreement on what the principle of rule of law means or should mean, although the concept has frequently been the subject of academic scrutiny.[373] Fueller and Raz build on the basic idea that the rule of law should guarantee that the law is an effective tool for individuals.[374] In some sense, this implies that the rule of law supports individuals in establishing their control by protecting procedural and substantive safeguards such as stability, openness, clarity, etc. This basic definition indicates that human rights alone are not sufficient for the empowerment of an individual. To achieve effective protection, the rule of law is indispensable. Thus, the rule of law serves as a concept that supports materialisation of human rights.

However, the rule of law can be also seen as a stand-alone concept. Lautenbach's definition of the rule of law stresses its *per se* value. The definition focuses on two key elements: the control of power and legality.[375] In relation to the first element, the rule of law is concerned with the balance between the establishment of order and the control of governmental power.[376] Regarding the second, legality

---

366 Case C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn* [2004] ECLI:EU:C:2004:614, para. 12.
367 European Data Protection Supervisor, 'Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology' 12.
368 Daniel J. Solove, *The Digital Person* (New York University Press 2004) 49.
369 Ibid.
370 Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International 2002).
371 Leonhard Den Hertog, 'The Rule of Law in the EU: Understandings, Development and Challenges' (2012) 53 Acta Juridica Hungarica 204, 205.
372 In the EU the rule of law is clearly present in the primary law as well in the court's jurisprudence but it is mostly focused on two areas: first, the monitoring and enforcement of EU values and principles in the 'backsliding' Member States or second, the EU's own adherence to the basic tenets of the rule of law. Dimitry Kochenov, Amichai Magen and Laurent Pech, 'Introduction: The Great Rule of Law Debate in the EU' (2016) 54 Journal of Common Market Studies 1045.
373 Spencer Zifcak, *Globalisation and the Rule of Law* (2005) 11-12.
374 Ibid., 20.
375 Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press 2014) 20.
376 Ibid.

demands that government keeps to the law and governs through law.[377] As Lautenbach puts it, the rule of law deals with the way in which the authority uses its power.

In the discussion on the rule of law, not only public authorities are of interest: similar arguments apply to various forms of strong organisational power, e.g. dominant actors in the private sector. For all those forms of institutional power, the rule of law requires a system in which rules are subject to Fueller and Raz's criteria, i.e., they support individuals in establishing their control by safeguarding procedural and substantive safeguards. Of course, in the private sector the sources of rules and the means of interpretation will be different. Nevertheless, the rule of law should also be maintained in private relations if they entail asymmetries of power.

Other forms of strong organisational power such as private, commercial organisations are of particular interest for individual rights in the big data era. '*Big data sensors and big data pools are predominantly in the hands of powerful intermediary institutions, not ordinary people.'*[378] Corporate entities are privileged at the expense of ordinary individuals. Moreover, new technologies can be so powerful and self-managing that they replace governments or organisations as instruments of governance.[379]

Richards and King described this situation as a 'power paradox' in which the power shifts from an individual to companies.[380] Technological development should in no way diminish the significance of the rule of law, which expresses a founding contract between those who govern and those who are governed.[381] As business players have become the real decision-makers, they should also adhere to those principles. Crawford and Schultz propose a big data due process to guarantee the rule of law in the data-driven decision-making process.[382] Data-driven decision-making that bears consequences for individuals must be preceded – at a minimum – by notice and the opportunity for a hearing on the matter before an impartial adjudicator.[383] Private actors should adhere to the same conditions for deprivation of a liberty or property right as the government does.[384]

3.2.8. Freedom to do business

In Article 16 of the Charter, which stands alongside the provisions on the right to the protection of privacy and intellectual property in Chapter 2, the EU legislator granted a constitutional tone to the freedom to conduct business.[385] As the Charter's explanatory memorandum elucidates, Article 16 guarantees the freedom to contract, which is an indispensable part of relations between private actors on the data market.

---

[377] Ibid.
[378] Lokke Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' 18.
[379] Also, more and more rules are replaced with the technology management, e.g. road safety will be secured by on-board vehicle technologies rather than by the provisions of road traffic laws or the highway code. See also Roger Brownsword, 'In the Year 2061: From Law to Technological Management' (2015) 7 Law, Innovation and Technology 1, 4.
[380] Richards and King (2013).
[381] Roger Brownsword, 'Technological Management and the Rule of Law' (2016) 8 Law, Innovation and Technology 100.
[382] Kate Crawford and Jason Schultz, 'Big Data and Due Process - Toward a Framework To Redress Predictive Privacy Harms' (2014) 55 BCL Rev. 93, 124.
[383] Ibid., 111.
[384] Ibid.
[385] Xavier Groussot, Gunnar Thor Pétursson and Justin Pierce, 'Weak Right, Strong Court - The Freedom to Conduct Business and the EU Charter of Fundamental Rights' in Douglas-Scott and Hatzis (eds), *Research Handbook on EU Law and Human Rights* (Edward Elgar Publishing Ltd 2017) 4.

The CJEU and national (constitutional) courts have only interpreted this provision on rare occasions, therefore the scope remains unclear. In relation to the data-driven economy, an illustrative example is the Belgian case in which private undertakings active in the health sector brought a claim on the basis of Article 16. They disputed the establishment of a public eHealth platform aimed at ensuring a secure exchange of personal health data between the undertakings. The Belgian court held that considering the nature of the tasks given to the eHealth platform and the sensitive nature of the data processed by the companies, the limitations to the freedom to do business should not be considered unreasonable or disproportionate.[386]

In recent years, protection of human rights has become more prominent on the EU level, and the CJEU has strengthened its role as an adjudicator on fundamental rights.[387] In cases related to data protection in particular, the Court has established itself as an advocate of individual rights.[388] In the recent case law, the balance between the freedom to conduct business and individual protection has tilted towards the latter. For example, in the *Google Spain* case, the Court claimed that *'[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.'* This starting point allowed the CJEU to perceive the 'interests' of data controllers as something less valuable than data subjects' fundamental rights.[389] While from an individual's perspective the decision was welcome, the Court's approach has also been criticised as too easily disregarding business interests.[390] As the right to conduct business aims to establish a smart, sustainable, and inclusive EU economy, it is not surprising that some have suggested more seriously taking Article 16 into account.[391]

3.3. EU secondary law

3.3.1. Introduction

As explained above, secondary law is a specific manifestation of more general fundamental principles of EU law. It builds on the foundation set in the Treaties and the EU Charter. The practical value of secondary law sources is that they are more precisely defined and thus more easily implemented than primary sources.

EU secondary law comprises unilateral acts such as regulations and directives that enable the EU to exercise its powers.[392] These are dependent on the primary law. Therefore, to be valid, they need to be consistent with the acts and agreements which take precedence.[393] In addition, they should be read in conjunction with primary law.

---

[386] Grondwettelijk Hof (Belgian Constitutional Court) No. 29/2010.
[387] Búrca, 26.
[388] Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23 Maastricht Journal of European and Comparative Law 812.
[389] Miquel Peguera, 'The Shaky Ground of the Right to Be Delisted' (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 507, 553.
[390] Ibid.
[391] European Union Agency for Fundamental Rights and Union, 'Freedom to Conduct Business - Exploring the Dimensions of a Fundamental Right' (2015) 51.
[392] Catherine Barnard and Steve Peers, *European Union Law* (Oxford University Press 2017) 104.
[393] <http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf> accessed 14 June 2018.

Although EU and MSs' national courts are the ultimate interpreters of the EU secondary law, in practice the opinions of MSs' data protection authorities and its EU counterpart, Article 29 Working Party's (the European Data Protection Board from 25 May 2018),[394] are highly influential. This thesis draws on many of these findings, opinions, guidelines and guidances. However, it should be kept in mind that only few of them have been tested in court, meaning that these documents are neither hard facts nor free of controversies.

The analysis in this section is an endeavour to identify secondary EU law sources that protect individuals in the data-driven economy. For the sake of simplicity, the analysis only considers those that are *prima facie* relevant. The selection is limited to four domains: data protection (including ePrivacy), cyber security rules, competition, and consumer protection.

3.3.2. Data protection law

The EU data protection law is a fragmented legal area entailing a number of legal acts.[395] This section focuses on those that play a role in protecting an individual in the data-driven economy. The key source is the 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, or GDPR).[396] As the name explains, the regulation covers any type of data processing with the objective of personal data protection. Furthermore, ePrivacy rules stipulated in the directive on privacy and electronic communications pursue the same goals, but they are focused on the area of electronic communication.[397] Sections 3.3.2.1 and 3.3.2.2 address these two acts, respectively.

3.3.2.1. General data protection

The GDPR was adopted to replace the outdated EU data protection directive.[398] Taking the form of a European regulation, the GDPR is binding in its entirety and directly applicable in all member states.[399,400] The GDPR rules can be divided into two large groups: 1) protection-oriented rules that tie

---

[394] The Article 29 Working Party was an advisory body made up of a representative of each EU Member State, the European Data Protection Supervisor and the European Commission. On 25 May 2018 it was formally replaced by the European Data Protection Board (EDPB).

[395] In the area of freedom, security and justice, a separate legal act imposes rules on data processing by police and judicial authorities. Handling of personal data by the public-sector bodies is regulated by a specific data protection regulation which only pertains to the EU institutions.

[396] *Supra* n 32.

[397] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L 201. This directive is soon to be replaced with a regulation. See Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final. See section 3.3.2.2. for the explanation of the relation between the area of ePrivacy and general data protection.

[398] *Supra* n 26.

[399] Article 288 of the Treaty on the European Union. That being said, the GDPR does allow Member States to legislate on data protection matters on numerous occasions, e.g., where the processing of personal data is dependent on a legal obligation, relates to a task in public interest or is carried out by a body with official authority. Bird & Bird, 'Guide to the General Data Protection Regulation' (2017) 1 <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> accessed 15 June 2018. Also, a number of articles state that their provisions may be further specified or restricted by a Member State law. In addition, in some sectors the GDPR may be preceded by sector-specific rules. Typically, this is the case for highly regulated sectors, such as health and financial services.

[400] What would happen if the national provisions would diverge but this would be in conflict with the GDPR? Then the regulation would apply directly, if the relevant provisions are sufficiently clear and precise. Gabriela Zanfir-Fortuna 'A

entities which use data for their commercial purposes, and 2) control-granting provisions that aim to give rights to data subjects who are the ultimate source of personal data. Before these two aspects of data protection law are discussed in sections 3.3.2.1.2 and 3.3.2.1.3, section 3.3.2.1.1 shortly describes personal data, which is the artefact on which the GDPR focuses and which it seeks to protect.

3.3.2.1.1. Personal data at the heart of data protection law

The main object of concern of data protection law is not an individual but her data. It has been shown that, in the same way as someone's body or mind, data is an essential part of individual identity.[401] Hence, by protecting personal data, we also safeguard an individual.

The majority of business models in the data-driven economy use personal data, which means that they directly or indirectly impact natural persons. The use of personal data varies in intensity and scope. Some commercial actors only perform personal data analytics as an ancillary activity,[402] while others use the data throughout their value chain and are closely involved in its collection, storage, and transfers.[403] Business models that involve data-driven decision-making are in principle more likely to affect an individual than those that visualise data, for instance.

Regardless of the level of interference, using personal data will trigger the applicability of data protection regulations. It is not always easy to define what personal data is. Cookies[404] and IP addresses[405] are two border-line examples. However, a solid understanding of the concept of personal data is critical to assess the degree of an individual's protection.[406]

The definition of personal data according to the GDPR (Article 4) contains four main elements: 'any information', 'relating to', 'an identified or identifiable', and 'natural person'.

'Any information' means that the information can be available in whatever form, can be either objective or subjective, and may contain various facts not necessarily related to someone's personal life.[407] The most open part of the definition is 'relating to', which explains the connection between an individual and his data. The Article 29 Working Party explains that information may relate to a person

---

million dollar question, literally: Can DPAs fine a controller directly on the basis of the GDPR, or do they need to wait for national laws?' (p*dpEcho*, 8 December 2016) <https://pdpecho.com/tag/direct-applicability-of-the-gdpr/> accessed 3 June 2018.

[401] Lambiotte and Kosinski demonstrate that showing how pervasive records of digital footprints, such as Facebook profile, or mobile device logs, can be used to infer personality, a major psychological framework describing differences in individual behavior. R Lambiotte and M Kosinski, 'Tracking the Digital Footprints of Personality' (2014) 102 Proceedings of the IEEE 1934.

[402] For example, the retail sector can greatly benefit from the big data analytics, especially if it is used within the supply chain process to boost profitability and to shape consumer price perception. McKinsey, 'Consumer Marketing Analytics Center' (2012) 6 <https://www.mckinsey.com/~/media/mckinsey/industries/retail/how we help clients/big data and advanced analytics/cmac creating competitive advantage from big data.ashx> accessed 3 June 2018.

[403] Acxiom Corporation is a marketing technology and services company with offices in the United States, Europe, Asia, and South America. Acxiom offers marketing and information management services, including multichannel marketing, addressable advertising, and database management. Acxiom collects, analyses, and parses customer and business information for clients, helping them to target advertising campaigns, score leads, and more. <http://www.acxiom.com/about-acxiom/> accessed 3 June 2018.

[404] For a detailed study see Frederik J Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' (University of Amsterdam 2014).

[405] See Breyer Case C-582/14, ECLI:EU:C:2016:779, 19 October 2016.

[406] To illustrate the issue: if a dynamic IP address is not considered personal data, the individual using the address enjoys limited communication privacy. See for example Benedik v. Slovenia App no 62357/14 (ECtHR, 24 April 2018).

[407] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) 25.

because of one of three elements: a content element, a purpose element, or a result element.[408] The same information may relate to individual XY because of the 'content' element (the data is clearly about XY), to XX because of the 'purpose' element (the data will be used to treat XX in a certain way), and to YZ because of the 'result' element (the data is likely to have an impact on the rights and interests of YZ).[409]

In general, the EU data protection authorities tend to adopt a wide definition of personal data.[410] For instance, IP addresses are in principle considered personal data,[411] although this may seem at odds with the basic definition of personal data.[412] However, it has been argued that the broader interpretation is indispensable to adequately respond to the challenge of extensive online data collection and processing, particularly in relation to behaviour advertising.[413] Advertisers create buyer profiles to determine consumers' shopping habits. Although the profiles do not directly relate to an individual person, instead representing an imaginary buyer, they are considered personal data when they are created with the purpose of treating an individual in a certain way or when they are likely to have an impact on an individual.

On a similar note, it is important to stress the concept of identifiability and its relevance for the data-driven economy, particularly due to the increasing importance of data analytics. In practice, data is often processed in an anonymised form. By anonymising personal data and processing only non-identifiable information, companies are exempted from data protection rules.[414] Sidestepping data protection rules can be problematic for two reasons. First, absolute anonymisation is never possible,[415] whereas re-identification is increasingly easy to achieve. Second, processing of anonymised data does not come without risk.[416] For example, it is possible to discriminate against a group of persons based on the results of aggregated, anonymised data.[417]

Some categories of personal data require special protection. These are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; genetic and biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation (Article 9(1)). As a general

---

[408] Ibid., 10.
[409] Ibid.
[410] Ibid.
[411] The CJEU case law also seems to support this reasoning. In *Scarlet v. Sabam* the Court balanced between three fundamental rights and freedoms: freedom to conduct business, right to property and right to data protection. In relation to the latter It held that *"… IP addresses are protected personal data because they allow those users to be precisely identified."* In *Breyer* the Court came to the same conclusion about dynamic IP addresses: they can be personal data if the internet service provider has the (access to) information that can be linked to addresses and allows for identification of individuals. Case C-582/14, *Breyer*, ECLI:EU:C:2016:779, 19 October 2016, para. 41-45; C-70/10 *Scarlet v. Sabam*, ECLI:EU:C:2011:771, 24 November 2011.
[412] For a critical analysis of the issue see Gerrit-Jan Zwenne, 'Diluted Privacy Law' (2013) <https://zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-Diluted-Privacy-Law-inaugural-lecture-Leiden-12-April-2013-ENG.pdf> accessed 3 June 2018.
[413] Frederik J Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347.
[414] Oostveen (2016).
[415] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.
[416] Ibid.
[417] Custers (2004) 172. Also see Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy and Technology.

rule, processing of data related to health is prohibited, but the GDPR allows for certain exceptions, for example explicit consent of a data subject[418] or substantial public interest (Article 9(2)).

The concept of sensitive data has faced some criticism. It has been argued that the group of characteristics that fall under the definition was chosen arbitrarily and that many other types of data can also reveal highly sensitive information about an individual.[419] Moreover, in the data economy, longitudinal and combined data sets – also called a comprehensive digital identity – play a significant role.[420] This data is not especially protected, although it can be highly revealing about individual circumstances.[421]

The GDPR tends to resolve some of these drawbacks. The regulation moves towards an expansive definition of personal data capturing cookies, IP addresses, web beacons, and other tracking technologies when used to track an individual.[422] The adopted text also introduces some new categories of sensitive personal data, e.g. genetic data.[423]

3.3.2.1.2. Protection-oriented duties of commercial data users

3.3.2.1.2.1. Definitions of data users

The rigour of data protection will often depend on the specific behaviour of those that use data. Therefore, it is important to understand how these users are regulated by exploring their protection-oriented duties.

The GDPR establishes a unique system of data users, splitting those that process data into two large groups. Based on the level of their autonomy, they are either controllers or processors. The line between the two groups is thin, and since the data economy is known for its diversity, it is not always clear who is a controller and who is a processor.[424] The final decision should be based on the actual relationship and not on contractual arrangements.[425] In most cases, data economy actors are considered data controllers, and consequently they are subject to all relevant obligations provided by data protection laws.[426]

According to the GDPR, a data controller is a natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (Article 2). In general, its main responsibility is to implement appropriate technical

---

[418] As the most relevant exception. Nadezhda Purtova, Eleni Kosta and Bert-Jaap Koops, 'Laws and Regulations for Digital Health' in Samuel A Fricker, Christoph Thuemmler and Anastasius Gavras (eds), *Requirements Engineering for Digital Health* (Springer 2014) 52.
[419] Kristina Irion and Giacomo Luchetta, 'Online Personal Data Processing and EU Data Protection Reform' (Centre For European Policy Studies Brussels 2013) 42.
[420] Ibid.
[421] Ibid.
[422] Olswang, 'EU Data Protection Reform: Where Are We – and What Can You Do to Prepare? '.
[423] Ibid.
[424] Seda Gürses and Joris Van Hoboken, 'Privacy After the Agile Turn' in Jules Polonetsky, Omer Tene and Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017) 395.
[425] Eduardo Ustaran and International Association of Privacy Professionals, *European Privacy: Law and Practice for Data Protection Professionals* (International Association of Privacy Professionals (IAPP 2012) 77.
[426] Cristina Dos Santos and others, 'LAPSI 1.0 Recommendation on Privacy and Data Protection' 14 <http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366> accessed 3 June 2018.

and organisational measures to ensure and to perform processing in accordance with the GDPR, i.e., by adhering to privacy principles and respecting data subject rights (Article 24).

The GDPR defines a data processor as a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller (Article 2 of the GDPR). Under the GDPR, data processors have a number of direct obligations: implementation of technical and organisational measures, notification of the controller without undue delay of data breaches, and the appointment of a data protection officer, if the nature of data processing requires it. If a processor engages a sub-processor, the latter should adhere to the same requirements.[427] Article 28 of the GDPR specifies how the processing of personal data by a processor should be governed in a contract, providing a number of mandatory provisions. *De facto* personal data protection often depends on this translation of the principles and obligations from the GDPR into commercial agreements between controllers and processors. In the data economy, a processor is typically an external entity specialised in data analysis to which the controller outsources certain tasks. In a relationship between a controller and a processor, the latter is often the dominating party. For example, a European small or medium enterprise as controller is much weaker than a global processor such as Dropbox. The negotiating power shifts to the processor's side, which can affect the freedom of contracting and result in less favourable contractual clauses for the controller.

3.3.2.1.2.2. Protection principles for personal data users

Data protection rules that apply to personal data users can be summarised in five key principles: (1) transparent, lawful, and fair processing; (2) specification and limitation of the purpose; (3) data minimisation and storage limitation; (4) accuracy, integrity, and confidentiality of personal data; and (5) accountability. The principles aim to establish boundaries for data processing and offer guidance to data controllers and processors to handle personal data in a legitimate and responsible way.

The first principle is three-fold. First, it requires transparent data processing, which means that any information addressed to the public or to the data subject is concise, easily accessible, and easy to understand, and that clear and plain language and, where appropriate, visualisation is used (Recital 60 of the GDPR).[428] In other words, the transparency requirement translates into being aware of some key aspects of data processing.[429] Second, the principle requires that data be processed lawfully. Article 6 of the GDPR establishes five legal bases for lawful processing: (a) data subject has unambiguously given her consent to processing; (b) processing is necessary for the performance of a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; and finally, (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data is disclosed. The final part of the principle is fairness. The GDPR does not define fairness, but it can be linked with numerous procedural safeguards that should, as a whole, constitute fair processing of data.[430] However, focusing entirely on the procedural safeguards

[427] See Chapter IV of the GDPR.
[428] Custers and Ursic, 'Worker Privacy in a Digitalized World under European Law' 339.
[429] Ibid.
[430] Ibid.

to achieve fair processing may risk disregarding the substantive side of fairness and actually departing from the objectives of the GDPR and broader EU law.[431]

In the data-driven economy, where personal data is commonly used for secondary purposes, the bases under (a) and (f) have proved to be most useful.[432] Individual consent (a) is a basis that inhibits a higher level of a data subject's independence and control. Unambiguous consent presupposes that a data subject has full understanding of the consequences of his approval. However, consent is the legal basis that can be easily diluted. For example, difficult-to-read privacy policies obscure which data is being collected and for which purposes. In turn, consent becomes a merely formalistic step.[433] Besides consent, a legitimate interest of a data controller (f) is likely to be used as a legal basis. Legitimate interest of a commercial actor will suffice if it outweighs the importance of the right to data protection. Data protection is considered a fundamental right, which means that the business side will usually have difficulty proving that its interest 'wins' over privacy.[434] The Article 29 Working Party takes a more balanced approach in its opinion. It states that when interpreting the scope of Article 6(f), it is necessary to ensure the flexibility for data controllers in situations where there is no undue impact on data subjects.[435] However, it is important that data subjects be provided with sufficient legal certainty and guarantees which prevent misuses of this open-ended provision.[436]

The principle of purpose limitation in article 5(b) is significant for the modern data economy, in particular for those controllers that actively *re*use personal data. It requires that the purposes for which personal data is collected be specified and that the data only be used for these purposes.[437] Any secondary data use, unless stipulated at the moment of data collection, is in principle prohibited.

This principle prevents controllers from exercising too much freedom regarding individuals' personal data. Controllers have to determine the purposes of data processing before the processing of data starts.[438] The data can only be used for a purpose which is compatible with the one for which it was collected. Such prior determination of purposes creates a sense of certainty and transparency, and enhances data subjects' control over their personal data.

---

[431] Ibid.
[432] Santos and others, 'LAPSI 1.0 Recommendation on Privacy and Data Protection' 25.
[433] Schermer, Custers and van der Hof (2013).
[434] Santos and others, 'LAPSI 1.0 Recommendation on Privacy and Data Protection' 26.
[435] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) 50. In *Breyer* the CJEU followed Article 29 working party's views. Case C-582/14, *Breyer*, ECLI:EU:C:2016:779, 19 October 2016, para. 60-63.
[436] The opinion refers to Article 7(f) of the DPD, however, the provision is identical to the one in 6(f) of the GDPR. As regards other legal bases, many of them cannot be used in practice due to the specific nature of the data economy. As Article 29 Working party notices, Article 6(b) must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. For example, the provision is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on a clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services. Also, it is very unlikely that reuse would be legitimated by a data subject's vital interest or general public interest. Both options have limited application. First, the phrase 'vital interest' appears to limit the application of this ground to questions of life and death. Second, the notion of 'general public interest' refers to public tasks that are assigned to an official authority or that are imposed on a private part by a public body. As such they cannot be used to justify business goals. Ibid., 10 and 20. See also Olswang, 'EU Data Protection Reform: Where Are We – and What Can You Do to Prepare? '.
[437] Article 6(b) of the DPD.
[438] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' 15.

In practice, the principle of purpose limitation is difficult to enforce.[439] First, it is unlikely that all possible reuses can be defined or predicted in advance. This can be frustrating for data economy actors, as they might feel that the possibilities to exploit the collected data have been disproportionately restricted. As a response to the restraining provision, controllers have started using an open and indefinite language that lacks specificity, with regard to both the data the networks collect and how they use this data. For instance, Facebook's privacy policy from 2015 only identifies categories of purposes by using vague descriptions such as 'Provide, Improve and Develop Services', 'Promote Safety and Security', and 'Show and Measure Ads and Services'.[440,441] However, this may be seen as sidestepping the intention of the legislator, and the processing based on such a policy may be considered illegitimate.

To help data reusers assess whether using the data in another context is legitimate, Article 6(4) of the GDPR provides detailed guidance.[442] The judgement on the compatibility of processing should be based on the following criteria: (a) links between the purposes for which the data has been collected and the purposes of the intended further processing; (b) the context in which the data has been collected; (c) the nature of the personal data; (d) the possible consequences of the intended further processing for data subjects; and (e) the existence of appropriate safeguards. Another form of the compatibility assessment was proposed by the Article 29 Working Party in its opinion on purpose limitation. To determine the compatibility of data reuse, the Working Party suggested a combination of a formal and subjective assessment. The first one is focused on the comparison between the purposes provided by the controller and actual data reuse, and the second on the context and the way in which the purposes can be understood.[443]

Article 5(c) of the GDPR requires those that control data to observe that data remains relevant, not excessive in relation to the purpose, and kept no longer than necessary for processing. This provision is also known as the principle of data minimisation. Minimising the amount of personal data that is processed should decrease the risk of data breaches and data mishandling. Article 5(1)(e) stipulates that personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Both requirements, but in particular the one in Article 5(c), seem at odds with the information-rich society, which collects vast amounts of data because it might prove useful in the future.[444,445] To overcome this challenge, the GDPR foresees some exceptions to data minimisation when data is processed solely for archiving purposes in the public interest, or for scientific and historical research purposes or statistical purposes. Moreover, subject to implementation of appropriate technical and organisational measures, the

[439] Zarsky (2018) 1005.
[440] Alsenoy and others (2015) 14.
[441] van der Hof, Schermer and Custers (2014).
[442] Here, a parallel can be made with the breakthrough study by Helen Nissenbaum on a conceptual analysis of context integrity that can be used in some borderline cases. Helen Nissenbaum (2010).
[443] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation'.
[444] Irion and Luchetta (2013) 45.
[445] It has been claimed that in some sectors, e.g. in medicine or pharmaceutical sector, data minimisation can even undermine lifesaving research attempts. Medical Devices Privacy Consortium's position paper on proposed EU data protection regulation, October 2014 <http://deviceprivacy.org/activities/mdpc-position-paper-on-eu-proposed-general-data-protection-regulation> (accessed on 16 October 2015).

storage time may be longer.[446] However, authorities have already made clear that this principle should in its essence remain unchanged despite the growing big data sector.[447]

The GDPR also provides guidelines in terms of accuracy, integrity, and confidentiality of data. First, personal data must be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate regarding the purposes for which it is processed be erased or rectified without delay (Article 5(1)(d)). Second, precautions should be taken against risks of loss, unauthorised access, destruction, etc. of personal data (Article 5(1)(f)).[448] These requirements aim for better protection of personal data and fewer intrusions caused by improperly applied or used data. In the big data era, these principles prove highly relevant. Incomplete, incorrect, or outdated data, where there may be a lack of technical rigour and comprehensiveness to data collection, or where inaccuracies or gaps may exist in the data collected or shared, can not only lead to wrong conclusions but may also cause discriminatory outputs.[449]

The principle of accountability requires controllers to be responsible for their compliance with the GDPR's principles and to be able to demonstrate it (Article 5(2)). For example, they may adopt certain 'data protection by design' measures (e.g. the use of pseudonymisation techniques), run staff training programmes, and undertake audits.[450] Given the scope and the risk of data processing, they may need to conduct privacy impact assessments[451] or hire (a) data protection officer(s).[452] All in all, accountability seems to be one of the most influential concepts on the protection side of the data protection law. Commentators see it as a promising way to deal with the challenges presented by the increasingly globalised nature of information flows, which are typified by recent developments in the field of e-commerce, such as cloud computing, and various types of data reuse.[453]

---

[446] Article 5(e) of the GDPR.
[447] See for example Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017) 11.
[448] The upcoming NIS directive imposes additional security-related requirements. See Section 3.3.3. for more detail.
[449] Executive Office of the President (White House), 'Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights' (2016) 7 <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf> accessed 3 June 2018.
[450] Bird & Bird, 'Guide to the General Data Protection Regulation' (2017) 33 <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> accessed 3 June 2018.
[451] A privacy impact assessment (PIA) is is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. It is advisable for all data processing, but required in the cases where fundamental rights are at a greater risk. Article 35 of the GDPR.
[452] A data protection officer (DPO) is is an appointed individual who advises implications of Data Protection law and develops the company's privacy and data protection policies. Article 37 of the GDPR.
[453] J Alhadeff, B Van Alsenoy and J Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in D Guagnin, L Hempel and C Ilten (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012) 49.

3.3.2.1.3. Control-enhancing rights of data subject rights

3.3.2.1.3.1. Definition of data subjects

A key aspect of personal data is that it relates to identified or identifiable[454] natural persons or, in the data protection language, data subjects. Data protection law pays special attention to data subjects by granting them a set of rights and authorising them to invoke these privileges.

3.3.2.1.3.2. Data subject rights

Data subject rights, also referred to as micro rights,[455] subjective rights,[456] or control rights,[457] are at the heart of this thesis and are explained in more detail in Chapters 5-9. For reasons of coherence, a short summary is provided below.

The GDPR contains an extended catalogue of eight subjective rights that are split into three sections: (1) information and access to personal data, (2) rectification and erasure, and (3) the right to object and automated individual decision-making.

Being informed is critical to ensure that individuals can give valid consent and exercise other control rights (Articles 13 and 14). The right to information is not exhausted once data processing starts. In the course of the processing, a data subject has the right at any time to access that same information and some extra information (Article 15).

The second group of rights focuses on the possibility of erasure and rectification. The right to erasure, popularly known as 'the right to be forgotten', allows data subjects to seek the deletion of data and block further reuse when consent is withdrawn or when the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed (Article 17). Data subjects are also entitled to demand rectification[458] or restriction of data processing.[459] As part of this second section, the GDPR introduced a new right to data portability, which allows data subjects to obtain a copy of that data for further use and to transmit it from one provider to another (Article 20).

Finally, the GDRP grants data subjects the right to object to data processing (Article 21) and the right to not be subject to a decision based solely on automated processing (Article 22). In particular, this group of rights seeks to limit some negative effects of profiling by explicitly stipulating that both rights apply to data processing for the purposes of individual profiling.

Control rights may be restricted in some situations, e.g. due to reasons of national security or other important rationales (Article 23). Some rights may face additional limitations. For example, portability of personal data is only guaranteed if the data in question is processed by automated means and if the

---

[454] An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Article 4 (1) of the GDPR.
[455] Lynskey (2015) 181.
[456] Ibid., 180.
[457] Ibid., 230.
[458] Article 16 of the GDPR.
[459] Article 18 of the GDPR. This right to restriction replaces the provisions in the Data Protection Directive on 'blocking'. In some situations, it gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held in limbo whilst other challenges are resolved. Bird & Bird (2017) 30. See Chapter 1, section 1.5. for the reasons why this right was exluded from the scope of the thesis.

processing is based on a legal basis set up in a contract, or on an individual's consent (Article 22 (1)(a), (b)).

3.3.2.2. Protection of privacy in public communication networks (ePrivacy)

Contrary to the GDPR as summarised above, the ePrivacy directive is a *lex specialis*.[460] It applies to the matters that are not specifically covered by the GDPR.[461] More precisely, it provides a detailed regime for personal data processing in the public communication sector. In this way, the ePrivacy directive complements the data protection regime while bringing the innovation necessary to cover digital technologies.[462]

To a large extent, the ePrivacy directive's objectives correspond to the objectives of the GDPR. In addition to ensuring free movement of data, the directive lays down rules for safeguarding fundamental rights and freedoms, and in particular the right to privacy (Article 1(1)). To this end, the directive mandates security of processing, confidentiality, and deletion of data when no longer needed.

In contrast to the GDPR, the ePrivacy directive concerns all public communication network users and not data subjects specifically.[463] The term 'users' covers Internet service providers' customers irrespective of their legal personality or the subscriber-provider relationship.[464]

The directive splits personal data that flows through public communication channels into two groups. The first group contains traffic data. This data may be processed and stored when necessary for billing purposes. In case traffic data is used for marketing purposes, a user's or subscriber's consent is needed (Article 6). The second group of data contains location data and other types of data. This data can be only used if it is anonymised or with a user's consent (Article 9).

Another important provision that the ePrivacy directive entails is the so-called cookie rule (Article 5(3)). This provision was inserted in the directive as a result of the 2009 amendment. Cookies are small text files that a website sends to a user's browser when this user requests the website. First-party cookies are set by the website publisher itself, and third-party cookies are set by others, such as ad networks.[465] Third-party cookies enable ad networks to follow people around the web, which may lead to disclosures of their browsing patterns and personal interests. By requiring a consent from every user whose online activity is tracked by cookies, the ePrivacy directive effectively mandates an opt-in approach. Although the opt-in regime offers control to data subjects, it has received strong criticism for being practically unworkable.[466] Faced with multiple cookie consent requests, users no longer make

[460] Frederik J Zuiderveen Borgesius and others, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (2017) 23 <https://www.ivir.nl/publicaties/download/IPOL_STU2017583152_EN.pdf> accessed 17 November 2017.
[461] Andrej Savin, *EU Internet Law* (Edward Elgar 2017) 299.
[462] Ibid.
[463] See the definition in Section 1.4.
[464] Savin (2017) 300.
[465] Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 31.
[466] Commission, 'ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation - Final Report' (2015) 12 <https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>.

active, informed choices when confronted with a consent situation, but instead simply provide consent when asked to do so.[467]

The ePrivacy directive also regulates direct marketing (Article 13). It introduces an opt-in/opt-out regime for communicating marketing-related messages. The latter can only be sent if this is approved by the consumer or in the course of an existing business relationship, given that the consumer has an option to cease the communication (Recital 41).

The European Parliament is currently negotiating a new ePrivacy law, the ePrivacy regulation.[468] The proposal for the ePrivacy regulation has a wider scope and also covers users of the over-the-top service providers offering communications services such as VoIP or instant messaging such as Whatsapp and Skype.[469] In addition, the draft regulation tightens the criteria for the use of communication data and enhances the principle of privacy by design.[470] The first impression is that the ePrivacy Regulation offers better control over electronic communication data but the final outcome remains to be seen. In fact, some of the recent reiterations of the draft regulation revealed political tensions to water the level of privacy protection down.[471]

3.3.3. Cybersecurity provisions

At first glance, cybersecurity does not concern an individual because it focuses on the question of cyber resilience of infrastructure. However, some recent data breaches that compromised some massive personal databases have demonstrated that cybersecurity importantly adds to the protection of personal information and, consequently, an individual.[472]

In the EU, the regulation of the field has long been fragmented, ranging from economic internal market elements, fundamental rights, and citizens' freedoms to criminal cooperation and defence policy.[473] The EU cybersecurity strategy was first addressed in 2004 when the European Council requested a critical infrastructure cybersecurity strategy, which led to the development of the European Network and Information Security Agency (ENISA) and was followed by the European Programme for Critical Infrastructure Protection (EPCIP) in 2008.[474]

---

[467] Schermer, Custers and van der Hof (2013), 12.
[468] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final. See also the latest, revised Council's text from 19 October 2018 <https://iapp.org/media/pdf/resource_center/ePR_10-19-18_draft.pdf> accessed 27 December 2018.
[469] Helena Ursic, '"The bad" and "the good" of ePrivacy proposal' (*Leiden Law Blog,* 19 January 2017) <http://leidenlawblog.nl/articles/the-bad-and-the-good-of-the-eprivacy-regulation-proposal> accessed 3 June 2018.
[470] Ibid.
[471] David Meyer, Eprivacy repporteur furious over Austria's limited ambition (*IAPP Privacy Advisor, 2018*) <https://iapp.org/news/a/eprivacy-rapporteur-furious-over-austrias-limited-ambition/> accessed 19 August 2018.
[472] For example Tom Lamont, 'Life after the Ashley Madison affair' *The Guardian* (27 February 2016) <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked> accessed 3 June 2018; Sam Thielman, 'Yahoo hack: 1bn accounts compromised by biggest data breach in history' *The Guardian* (5 December 2016) <https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached> accessed 3 June 2018.
[473] Ramses A Wessel, 'Towards EU Cybersecurity Law: Regulating a New Policy Field' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 424.
[474] Scott J Shackelford and Scott Russell, 'Operationalizing Cybersecurity Due Dilligence: A Transatlantic Comparative Case Study' (2017) 67 University of South Carolina Law Review 15.

In 2013, the EC set the EU cybersecurity roadmap with the Communication on Cybersecurity Strategy for the EU. Primarily, the EC planned to realise the strategy with the network and information security (NIS) directive. The directive, which was adopted on 6 July 2016, marked a fundamental change in the scope and strategy of the EU cybersecurity rules.[475] Until recently, information security rules were focused either on the protection of subjective rights (e.g., data breach notification provisions) or on the deterrence of and retaliation against deliberate attacks (anti-cyberattacks regulations).[476] The NIS directive, in contrast, attempts to strengthen the public and private IT infrastructure as a whole by creating and introducing institutions and instruments such as expert organisations, certification regimes, and information systems.[477]

The main aim of the directive is a high common level of security of network and information systems within the EU so as to improve the functioning of the internal market. In line with this far-reaching objective, the scope of the directive is broad and can be applicable to a wide range of data users, including, e.g., social media providers or IoT system operators.[478]

The NIS directive aims to achieve its objectives by requiring the member states to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures such as energy and transport, key providers of information society services (e-commerce platforms, social networks, etc.), and public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities (Article 14 and Article 16 of the NIS directive). Also in relation to security, the proposed NIS directive requires market operators to prevent and minimise the impact of security incidents on their core services, and thus ensure their continuity. In other words, not only must the operator of, for instance, a remote medical device take preventive and defensive measures, it must also be able to continue functioning when incidents do occur. Furthermore, the directive imposes a duty to notify the competent authority about incidents having a significant impact on the security of the core services provided (Article 14(3) and 16(3)) and grants the competent authority the possibility to inform the public, or require public administrations and market operators to do so, when in the public interest (Article 14 (4)).

It should be borne in mind that the GDPR already contains a number of rules on security standards for processing of personal data. Notably, the obligation to notify authorities of breaches is part of the updated data protection regime (Articles 34 and 35 of the GDPR). However, the GDPR's notification provision has a limited scope. It requires a notification only if there is a *substantial* impact on the rights and freedoms of natural persons. In contrast, the NIS directive has a broader and more general effect,

[475] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1 (NIS directive).
[476] Thomas Wischmeyer, 'INFORMATIONSSICHERHEITSRECT: IT-Sicherheitsgesetz Und NIS-Richtlinie Als Elemente Eines Ordnungsrechts Für Die Informationsgesellschaft' (2017) 50 Die Verwaltung.
[477] Ibid.
[478] The subject matter, namely a network and information system, covers: (a) an electronic communications network (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by elements covered under the two bullet points above for the purposes of their operation, use, protection and maintenance. Article 3 of the NIS Directive.

as it seeks to improve security safeguards and the sharing of knowledge on cybersecurity threats.[479] This is why it also has potential to enhance the protection of personal data.

3.3.4. Competition law

As a general proposition, competition law consists of rules that are intended to protect the process of competition to maximise consumer welfare.[480] Competition law is concerned with practices that are harmful to the competitive process, in particular with anticompetitive agreements, abusive behaviour by a monopolist or dominant firm, mergers, and public restrictions of competition.[481] Competition has gained central importance in the EU as one of the most powerful tools the authorities have to restore consumers' welfare.[482]

The EU competition law framework is highly complex. Key provisions are contained in Articles 101 (prohibition of anticompetitive agreements) and 102 (prohibition of abuses of the dominant position) of the TFEU and in two regulation: Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), and Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices. In addition, the European Commission's communications and the CJEU's case law have a significant impact on the interpretation of the law.[483]

Competition law settles the conditions for a free and unrestricted access to the market, and this should also be the case on the market of (big, personal) data. Today, data is considered an important asset in the same way as intellectual property (IP), goodwill, or intellectual capital. On the Internet, personal data plays the role of a digital currency. For instance, social network users agree to exchange their personal data for access to a digital service. Later, this same data may be sold to advertisers.[484] Through control of data, companies that operate on two-sided markets generate profit and accumulate power. If one of these companies acquires a dominant position, this might result in undesired consequences such as tying, anticompetitive agreements, or exploitation of competitors.[485]

---

[479] Gabe Maldoff, 'NIS + GDPR = A New Breach Regime in the EU' IAPP Privacy Tracker (22 December 2015) > <https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/> accessed 3 June 2018.
[480] Richard Whish and David Bailey, *Competition Law* (Oxford University Press 2012) 1.
[481] Ibid., 3.
[482] Ibid., 19.
[483] An interested reader should refer to Craig and De Burca (2015); Whish and Bailey (2012); Federico Ferretti, *EU Competition Law, the Consumer Interest and Data Protection - The Exchange of Consumer Information in the Retail Financial Sector* (2014).
[484] Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088> accessed 3 June 2018.
[485] EDPS pointed at the difficulty of clearly defining the data market. 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' 28. Namely, if there is no market definition, regulators cannot determine a dominant position or monopoly. Consequently, they have no basis to claim an abuse of dominance, which is one of the fundamental competition law breaches. Also, they would experience difficulties with proving anticompetitive agreements or mergers. For example, online firms were able to convince some (US-based) courts that there was no product market for free services like search, which painted a false picture of the situation on the market. Maurice E Stucke and Allen P Grunes, 'No Mistake About It: The Important Role of - Antitrust in the Era of Big Data' [2015] University of Tennessee Legal Studies Research Paper 7.

The importance of (personal) data for competition on the digital market has been assessed very few times. In the Google/DoubleClick case,[486] the EC examined whether a mere combination of DoubleClick's assets with Google's assets, in particular the databases that both companies had or could develop based on customer online behaviour, could allow the merged entity to achieve a position that could not be replicated by its competitors.[487] The Commission also reviewed the case of a merger between TomTom/Tele Atlas.[488] The business goal of that merger was to enable TomTom to reuse (integrate) and sell the information acquired from its new business partner Tele Atlas (the merged company).[489] TomTom and Tele Atlas tried to defend the merger with an efficiency claim, arguing that that data in the form of feedback from TomTom's large customer base would allow the merged firm to produce better maps faster.

Both the Google/DoubleClick case and the TomTom/Tele Atlas case were cleared. Nonetheless, the fact that a lengthy and costly procedure was initiated confirms the seriousness of the situation and the likelihood of its negative impact on competitiveness and consumer welfare in the EU. In fact, with the increasing importance of big data, its legal impacts on personal data protection have been progressively discussed in academia and practice.[490] For instance, the EU data protection supervisor (EDPS) argued that a more serious approach to the role of personal information in competition law would encourage the usage of privacy-enhancing services (and add to consumer welfare).[491] Furthermore, the German antitrust watchdog (the Bundeskartellamt) recently initiated a proceeding against Facebook Inc., USA, in relation to its terms of service related to the use of user data.[492] They accused Facebook of abusing its dominant position in the market for social networks in violation of Article 102 TFEU. Specifically, the Bundeskartellamt claimed that Facebook was using its position as the dominant social network '*to illegally track users across the Internet and reinforce its might in online advertising*'.[493]

Regardless of these advances in practice, authorities remain hesitant to see data privacy as an aspect of competition law. Competition concerns should only be taken into account when the use of such data has adverse economic consequences – not adverse consequences for data protection alone.[494] In cases where (personal) data use is a subject of the competition law discussion, it is important that authorities

---

[486] *Google/Double Click* (Case COMP/M.4731) C(2008) 927 [2008] OJ C 184.
[487] Julia Brockhoff and others, 'Google/DoubleClick: The First Test for the Commission's Non- Horizontal Merger Guidelines' [2008] Competition Policy Newletter 53.
[488] TomTom/TeleAtlas (Case COMP/M.4854) C(2008) 1859 [2008] OJ C 237/8.
[489] TomTom integrates the navigable digital databases it purchases from Tele Atlas into the navigation software the company produces. The integrated product (software and database) is then either included in the personal navigation devices that TomTom itself sells to end-consumers or is sold to other manufacturers of navigation devices for inclusion in their devices. TomTom/TeleAtlas (Case COMP/M.4854) C(2008) 1859 [2008] OJ C 237/8, para 15.
[490] Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 Yale Law Journal 710; Geradin and Kuschewsky.
[491] The EDPS argues that '… *if companies are compelled to be transparent about the true value of the personal information which they collect, and market analyses take this value into account as part of competition decision, firms might begin to seek competitive advantages by reducing the periods over which information is retained or by providing a 'clear-my-data' button*.' 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' 33.
[492] Press Release on Preliminary assessment in Facebook processeding <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html> accessed 3 June 2018.
[493] Nicholas Hirst, 'Facebook's data collection faces antitrust charge in Germany' *politico.eu* (19 December 2017) <https://www.politico.eu/article/facebook-data-collection-could-be-an-antitrust-abuse-in-germany/> accessed 3 June 2018.
[494] Darren S Tucker and Hill B Wellford, 'Big Mistakes Regarding Big Data' [2014] The Antitrust Source.

understand both competitive benefits and risks of data-driven strategies. Sometimes, a data-driven merger may provide sufficient scale for smaller rivals to effectively compete, while at other times, data may be used primarily as an entry barrier.[495]

3.3.5. Consumer protection law

Consumers are an important factor in the data economy, which typically takes place on the Internet. The more consumers' activities are carried out online, the greater is the need for their protection.[496] Threats to consumers usually come from fraud and problematic business practices. The law seeks to protect consumers by safeguarding the following three interests: fair trading, privacy of consumer information, and morality (e.g. protection of minors against offensive content).[497] The second interest is addressed by data protection law, the third by specific rules on protection of minors or by fundamental rights, and the first one is typically a matter of consumer protection law. In Europe, the main body of consumer protection law consists of the consumer rights directive,[498] the unfair terms directive,[499] and the unfair commercial practices directive.[500]

The EDPS argues that consumer protection law plays a visible role in the data-driven economy in particular in ensuring transparency and accuracy of information.[501] The UK regulator for markets and competition (CMA) has also embraced this position. In June 2015, it published a comprehensive opinion on the commercial use of consumer data[502] listing a number of business practices that are arguably disputable under consumer protection law. For example, according to the CMA, misrepresenting the privacy, security, or confidentiality of users' information – which could still be deceptive, even if the privacy policy or other small print is factually correct (for example, the consumer is told that data is collected to complete a purchase) – violates the provisions of fairness set down in the EU and UK national legislation.[503] In the literature, it has been argued that consumer protection law could complement data protection law by imposing extra obligations with regard to informing users about so-called 'free' services, unfair terms, unfair practices, and consumer vulnerability.[504]

---

[495] Stucke and Grunes (2015) 4.
[496] Savin (2017) 160.
[497] Ibid.
[498] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] L 304/64.
[499] Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts OJ [1993] L 95/29.
[500] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] L 149/22.
[501] European Data Protection Supervisor, 'Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability (Opinion 7/2015)'. See also Commission, 'A new European Consumer Agenda – Boosting confidence and growth by putting consumers at the heart of the Single Market' <http://europa.eu/rapid/press-release_IP-12-491_en.htm> accessed 3 June 2018.
[502] Competition & Markets Authority, 'The Commercial Use of Consumer Data' (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf> accessed 3 June 2018.
[503] Among others, CMA observes that (contrary to the Consumer rights directive) the Council directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts and its implementation act(s) applies whether or not the consumer pays with money – for example if the product is being provided in exchange for personal data. Ibid., 66.
[504] 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 8.

Along these lines, consumer law could be useful in addressing the risks imposed by data-driven business models, such as those in the IoT environment. For instance, Articles 5(1)(c) and 6(1)(e) of the consumer rights directive, which provide that consumers need to be informed in advance about 'the total price of the goods or services inclusive of taxes', could be applicable to the non-monetary exchanges in freemium models, in which consumers share their data in exchange for a service.[505] Moreover, Article 3(1) of the consumer contracts directive, which determines when a contractual term is unfair, could be useful to protect consumers' privacy interests and their freedom of expression, and to prevent the chilling effects of surveillance.[506] The directive defines as unfair a term that, contrary to the requirement of good faith, causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.[507] How this provision could protect individuals who share their data on the Internet can be explained with the example of an agreement between a mobile phone user and an app developer. In this contract, the app developer grants the consumer a license to use an app in return for which the consumer allows the developer, acting as a data controller, to collect location and usage data to provide advertising for as long as the app is installed.[508] While this exchange of consumer data for a licence can be legal under data protection law (the data subject has given her consent), it is not necessarily so under consumer protection law. Such a case could lead to a violation of the unfair terms directive. *'Allowing surveillance in exchange for the ability to switch an LED on or off seems like such a bad deal, that the 'requirement of good faith' has probably not been met.'*[509]

In principle, consumer protection law applies to economic transactions for money, not data.[510] In the past, personal data played only a small role in the process of amending the consumer law framework to meet the needs of the digital economy.[511] Instead, the EU focused on adjusting traditional consumer law instruments to digital services.[512] However, this is prone to change. The recent proposal for the directive on digital content (DCD) in Article 13 (2)(c) treats data exchanges as equal to monetary ones.[513] Besides the declaratory value of the provision, this explicit recognition of data as counter-performance also triggers direct application of other consumer protection rights such as the option for users to retrieve their data for free when they leave the service (and Article 16(4)(b) of the DCD).[514]

---

[505] Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' 9.
[506] Ibid., 12.
[507] Article 3(1) of the Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts OJ [1993] L 95/29.
[508] Michiel Rhoen, 'Big Data and Consumer Participation in Privacy Contracts: Deciding Who Decides on Privacy' (2015) 31 Utrecht Journal of International and European Law 51, 7.
[509] Ibid.
[510] Helberger, Borgesius and Reyna (2017) 12.
[511] Ibid., 8.
[512] Ibid., 8.
[513] 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. Article 3(1) of the proposed Directive gives exchange with data the same status as money*: 'This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data.'*
[514] Although the possibility that consumer law would address some data-driven contracts should be in principle encouraged, there is no perfect alignment between consumer protection and data protection law which may cause issues. For instance, the right to retrieve data may overlap with the right to withdraw. Also, in some cases, typical instruments of consumer protection (e.g., the right to return a product and demand money back) will not work when data is used as counter-performance. Helberger, Borgesius and Reyna (2017) 8.

3.4. Conclusions

This chapter answered the second research sub-question by examining the EU legal framework that applies to the data-driven economy and secondary data uses. It showed that EU law protects individuals through a number of provisions of primary and secondary law, which in many aspects complement each other. The body of law that adds to individual protection in the big data age has been evolving. Many key legal rules have recently changed (the new right to data protection in the EU Charter, the adoption of the GDPR) or are about to change (the proposal for ePrivacy regulation and the DCD).

Besides guaranteeing protection of individuals, these laws also grant mechanisms of control and empowerment for individuals. The idea of control is underlined by some fundamental rights provisions (e.g., dignity and privacy), but it materialises most evidently in the secondary law sources. Among them, data protection law certainly stands out. Two sets of data protection rules are directly linked to the concept of individual control: consent and data subject rights. The latest amendments of the EU data protection law through the GDPR brought no major changes in the system of consent, but they did substantially amend the section on data control rights. This makes them an interesting subject for further research, which is discussed throughout the following chapters.

4. CONTROL AS A CENTRAL NOTION IN THE DISCUSSION ON DATA SUBJECT RIGHTS

4.1. Introduction

Chapter 2 presented four values that are critical for individual well-being but can be undermined as a result of ubiquitous personal data collection, mining, and processing in the data-driven economy: *autonomy, privacy, transparency,* and *(market-)power symmetry*. As shown in the present chapter, one common denominator of all four values is the concept of *control over data*. The individual control over data is most directly reflected in the value of autonomy as an expression of individuals' self-determination and free will. Privacy, in particular informational privacy, also overlaps with the concept of (individual) control, especially when it is defined as the right to determine the use of personal information and flows – in other words, privacy as control over personal information.[515] Transparency is a necessary precondition for control, whereas power asymmetries grow out of imbalanced control distribution.

Chapter 2 also indicated that individuals' control in the data-driven economy is rather weak and some other groups of actors are in a considerably better position to exercise control over personal data. The data-driven economy has generated an environment in which the so-called data barons (i.e. large companies, government agencies, intermediaries) have a unique control over digital information, which is no longer counter-balanced by the control of other actors.[516] As was explained in Chapter 3, data protection law looks at data barons as data controllers. As the name indicates, controllers have the measures and power to control data. To prevent abuses, the law constrains their powers and imposes data protection duties. The unequal distribution of control among the actors in the data economy is further addressed by the GDPR provisions that aim to enhance data subjects' control. Chapter 3 highlighted two sets of data protection rules in the GDPR: those on consent and those on data subject rights.

Besides data subjects and controllers, there is a third group of actors also capable of exercising control over personal data use. This group is composed of data protection authorities and some other public bodies.[517] Some argue that the rigour of control that they exercise should increase in the upcoming years.[518] Namely, in the data-driven economy, data protection authorities rather than users have the technological knowledge to evaluate the risks of data processing and the access to adequate measures.[519]

Control appears to be a central notion for the discussion on data subject rights, but in data protection law it is poorly articulated. Before specific rights are analysed, the notion of control must be explored in more detail. To this end, the research sub-question addressed in this chapter is the following: *What does the notion of individual control entail and, specifically, how does it relate to the discussion on data subject rights*? (the third research question) By answering this question, this chapter serves as a

---

[515] Solove (2004) 77; Westin (2015).
[516] Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking The "notice and Consent" paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law and Security Review 643, 650.
[517] E.g. consumer protection authorities.
[518] Hijmans (2016) 497; Mantelero (2014) 657.
[519] Ibid., 647.

bridging section between the general part on the economic reality of the data-driven markets, and the more specific part on data subject control rights. The discussion on the notion of control is key to understanding the role of control rights in the data-driven economy and therefore serves as a basis for answering the key research question of this thesis.

The chapter is organised as follows. Section 4.2. analyses the notion of control by summarising how different scientific disciplines interpret it. Section 4.3. then explains what role the concept of control plays in the area of human and fundamental rights protection. Four fundamental rights that embody ideas of control are briefly explained: the right to property as the most apparent expression of individual control over something, the right to informational self-determination, the right to privacy, and the right to data protection. In section 4.4., the focus is on data protection law, which is described as a two-fold regulation that has strong potential in recognising and granting individual control over data. In particular, the idea of individual control is enshrined in provisions on subjective rights and consent. Due to the limited scope of this work, the notion of consent is not discussed in detail, whereas control rights, representing the core issue of this thesis, are analysed more thoroughly. Finally, section 4.5. explains the reasons why, in the data-driven economy, control is a challenging aspiration. Three groups of factors – technological, psychological and economic – are identified as common challenges to data subject control.

4.2. Roots of the term

4.2.1. Ordinary language and dictionary meaning

In ordinary language, control has two dimensions. It implies that someone is, first, aware of a situation and, second, able to influence it. The second building block of control, i.e., the ability to influence, is central to the dictionary definition of the word. The Concise Oxford Dictionary defines control as the power to direct and to influence.[520] Similarly, Merriam-Webster defines control as having power over or as exercising restraining or directing influence over someone or something.[521]

Dictionary explanations of control are broad, open to different interpretations, and context-dependent. In the context of the data-driven economy, for instance, control requires influence over three stages in a data value chain: data collection, analytics, and data-driven decision-making.[522]

4.2.2. Control in philosophy

The concept of control corresponds to three pivotal philosophical notions: free will, liberty and autonomy. These three notions are seen as values, that is ideals or beliefs shared by a society about what is good and what is not, and function as normative anchors of fundamental human rights and principles. As mentioned above, these values are critical for individual well-being but can be undermined in the data-driven economy. The sections below briefly describe what role the notion of control plays in relation to them.

---

[520] 'control', Oxford Living Online Dictionary <https://en.oxforddictionaries.com/definition/contro> accessed 4 June 2018.
[521] 'control', Merriam-Webster Online Dictionary <https://wwwwww.merriam-webster.com/dictionary/control> accessed 4 June 2018.
[522] Compare Westin (2015) 5, who similarly distinguishes three control stages - control of when, how and to what extend information is communicated.

Free will ensures that a process or a situation is up to, or controlled by, the agent.[523] Controlling the process requires true alternative possibilities. When this is the case, an agent also becomes morally responsible for what he does.[524]

A notion that is related to and sometimes overlaps with the concept of free will is that of individual liberty. In ordinary language, liberty refers to the quality or state of being free, and entails the power to do as one pleases, the freedom from physical restraint, the freedom from arbitrary or despotic control, and also the power of choice.[525] In philosophical discussions, liberty is often split into two subcategories: negative and positive freedom. 'Negative freedom' refers to freedom from interference, to the absence of something, whereas 'positive freedom' refers to what we are free to do and is thus associated with the presence of something. This something is typically described as self-mastery, self-determination, self-realisation, and, finally, control. The concept of positive freedom is often used in relation to data protection as a manifestation of individual self-determination and control.[526]

In general, autonomy is attributed to a person when this person has de facto *power and authority to* direct affairs of elemental importance to her life within a framework of rules (or values, principles, beliefs, pro-attitudes) that she has set for herself.[527] In other words, when agents have control, they should in principle have autonomy. However, agents can be deprived of their autonomy by brainwashing, depression, anxiety, or fatigue; and they can succumb to compulsions and addictions.[528] Thus, exercising control does not always translate to having full autonomy. An example can be found in the medical field: consent to share medical data signed by a mentally ill person demonstrates some control, but due to the person's special circumstances his control lacks true autonomy.[529]

In philosophical conceptualisations, control is closely related to some key values. If effective control is absent, values deteriorate too. In addition, effective control over data is linked with moral responsibility of data subjects for their actions regarding data. For instance, when control mechanisms such as consent do not translate to actual autonomy and free will, e.g. because of a data subject's inability to understand the process or because no true alternatives exist, then this affects the level to which a data subject can be held responsible.

4.2.3. Control in psychology[530]

Typically, psychologists define control as the ability of an agent to intentionally produce desired outcomes and prevent undesired ones.[531] Skinner stresses that a sense of control is a robust predictor of physical and mental well-being. In her framework, control is strongly associated with autonomy,

---

[523] Stanford Encyclopedia of Philosophy <https://plato.stanford.edu/entries/freewill/> accessed 4 June 2018.
[524] Harry G Frankfurt, 'Alternate Possibilities and Moral Responsibility' (1969) 66 The Journal of Philosophy 829, 830.
[525] Merriam-Webster Online Dictionary <https://www.merriam-webster.com/dictionary/liberty> accessed 4 June 2018.
[526] See for example Jeanne Pia Mifsud Bonnici, 'Exploring the Non-Absolute Nature of the Right to Data Protection' (2014) 28 International Review of Law, Computers & Technology 131, 138.
[527] Marina Oshana, 'Autonomy and the Question of Authenticity' (2007) 33 Social Theory and Practice 411.
[528] Stanford Encyclopedia of Philosophy <https://plato.stanford.edu/entries/personal-autonomy/> accessed 4 June 2016.
[529] Of course, the law mitigates this problem by requiring a valid consent which includes person conscience and understanding. See for example the Convention on Human Rights and Biomedicine (Oviedo Convention), Article 5 <https://rm.coe.int/168007cf98> accessed 15 August 2018.
[530] This section uses excerpts from the article by Helena U Vrabec and Iris van Ooijen, 'Does the GDPR Enhance Consumers' Control over Personal Data?: An Analysis From a Behavioural Perspective' (2018) Journal of Consumer Policy, 1-17.
[531] Ellen Skinner, 'A Guide to Constructs of Control 71(3)' (1996) 71 Journal of Personality and Social Psychology 549, 554.

self-determination, and perceived freedom.[532] Among the antecedents of control, Skinner lists information, choice, and predictability.[533]

A fundamental distinction in the literature on control is the one between actual and perceived control. This distinction is critical since experienced control (i.e., beliefs or experiences), rather than actual control, has psychological consequences.[534] In other words, changes in actual control will only have psychological consequences if the person's beliefs or experiences change. For example, a person may formally have the ability to exert increased control on the storage and distribution of her personal data by search engines, but if the process to prevent storage and distribution of this data is perceived as incredibly complex, then control is not experienced as such. Therefore, increased actual control may not result in experiences of self-determination and autonomy. On the other hand, the illusion of control entails that perceived control in a given situation is high, while in fact actual control may be low. For instance, a consumer may perceive that he has control over the extent to which his personal information is collected and distributed by a social network site because this website offers to alter its privacy settings.[535] However, by explicitly providing this possibility only for a part of the privacy settings, and leaving out other information (for instance, that the information will be distributed to third parties), the data collector creates a false sense of control and generates information asymmetry between itself and the individual. Although perceived control may increase in such a situation (along with experiences of self-determination and autonomy), actual control deteriorates.

The distinction between actual and perceived control is relevant to the discussion on control within law. When control is structurally not experienced as such, regulation will fail to empower consumers to control their personal data. Knowledge of the factors that stimulate perception of control may contribute to the development of policies that enhance consumer control and, consequently, their well-being. In principle, policies should encourage situations in which both perceived and actual control are present. However, Acquisti et al. write about a paradox that occurs with privacy enabling technologies (PETs).[536] Whereas PETs in theory lead to enhanced control (actual and perceived), the feeling of security conveyed by the provision of fine-grained privacy controls lowers concerns and

---

[532] Ibid., 550.

[533] Ibid., 555. This establishes an interesting parallel to data protection law. Consent provision, which is an important manifestation of individual control over data in data protection laws, requires that individual is informed about data processing, has the possibility to predict (to a reasonable degree) future data uses and is given a valid choice to either approve or disapprove data processing. Hence, psychological antecedents of control overlap with conditions for exercising control over personal data in the legal sense.

[534] See for example Jerry M Burger, 'Negative Reactions to Increases in Perceived Personal Control' (1989) 56 Journal of Personality and Social Psychology 246.

[535] In the aftermath of the data mining scandal in March 2018, Facebook decided to offer stronger privacy controls to individuals. '*In the coming months, privacy controls that are now in 20 places on Facebook's app will be merged into a single page, and will include what the company says will be easier-to-comprehend features that explain how the company is using a person's data, the company announced. […] Facebook also will create a page that makes it easier for people to download their data so that they can more clearly view what information the company collects about them*.' Elizabeth Dwoskin and Tony Romm, 'Facebook makes its privacy controls simpler as company faces data reckoning' *The Washington Post* (28 March 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/03/28/facebooks-makes-its-privacy-controls-simpler-as-company-faces-data-reckoning/?utm_term=.f330e90d2ba9> accessed 3 June 2018.

[536] Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4 Social Psychological and Personality Science 4(3) 340.

drives those provided with such protections to reveal more sensitive information to a larger audience.[537]

Psychological studies show that within the increasingly complex data economy, privacy by control is more an inspiration than a realistic goal.[538] The combination of bounded rationality, the tendency of consumers to attend to the online environment with only partial attention, and the increased (risk of) vulnerability and uncertainty that are associated with online data transactions cause consumers to surrender and disclose their personal data beyond what is desired.[539] On these grounds, the very possibility of control by the conventional figure of 'rational and autonomous agent' is seriously questioned.[540]

4.3. Individual control over data and fundamental rights

In the philosophical and psychological discourse the notion of individual control is closely related to some important values, such as self-determination, freedom, autonomy, and privacy. These values are normative anchors for the fundamental rights and principles enshrined in the EU primary law.

Just like the notion of control is integrated in the values, it is also reflected in the principles and rights that these values underpin.[541] For example, in relation to the right to data protection, control has been enshrined in the provisions of several legal treaties and fundamental documents, such as in the German Constitution, the ECHR as interpreted by the ECtHR, and, arguably, the US Constitution.[542] For this thesis, it is of particular importance to determine if/how control is addressed on the EU level, in particular in the EU Charter. Below, three rights from the EU Charter are explained in light of the underlying idea of control: the right to informational self-determination, the right to privacy and data protection, and the right to property. The right to informational self-determination is not explicated in the Charter but influenced its drafting process as an important source of inspiration.[543]

4.3.1. Control over personal data and the right to informational self-determination

Self-determination as a right is a fundamental issue in contemporary international law. It denotes people's legal right to decide their own destiny in the international order. In other words, it means removing illegitimate (foreign sovereign) powers and bringing control over government back to the genuine nation.[544] *Informational self-determination* embodies a similar idea of control, i.e. deciding

---

[537] Ibid.

[538] See for instance Bernadette Kamleitner and Vincent-Wayne Mitchell, 'Can Consumers Experience Ownership for Their Personal Data? From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints BT - Psychological Ownership and Consumer Behavior' in Joann Peck and Suzanne B Shu (eds) (Springer International Publishing 2018).

[539] See also Christophe Lazaro and Daniel Le Métayer, 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPT-ed 4, n 3, quoting A Acquisti and J Grossklags, 'What Can Behavioral Economics Teach Us About Privacy' in A Acquisti et al (eds), *Digital Privacy. Theory, Technologies, and Practices* (New York: Auerbach Publications, 2007).

[540] Ibid.

[541] Principles are fundamental truths or doctrines of law; comprehensive rules or doctrines which furnish a basis or origin for others; settled rules of action, procedure, or legal determination <https://thelawdictionary.org/principles/> accessed 4 June 2018. Rights are privileges that if challenged are supported in court <https://thelawdictionary.org/legal-right/> accessed 4 June 2018.

[542] Gabriel Stilman, 'The Right to Our Personal Memories: Informational Self-Determination and the Right to Record and Disclose Our Personal Data' (2015) 25 Journal of Evolution and Technology 14, 15.

[543] Hijmans (2016) 60.

[544] Karen Parker, 'Understanding Self-Determination: The Basics' (presentation at the First International Conference on the Right to Self-Determination, Geneva 2000) <http://www.guidetoaction.org/parker/selfdet.html> accessed 4 June 2018.

over the destiny of individual data and directing data uses. More specifically, this right provides individuals with the power to decide for themselves about issues of collection, disclosure, and use of their personal data.[545] The right to self-determination was first explicated in 1983 by the German Constitutional Court, which found its roots in the first article of German Basic Law (German Constitution) focused on protecting personality rights including human dignity.[546] In the landmark decision, the Court drew on the notion of self-determination to tackle the issue of privacy and integrity of IT systems in relation to population census.[547] The Court not only held that individuals should be protected against the unrestricted collection, storage, use, and transfer of their personal data, but also insisted that individuals were afforded the freedom to decide whether to engage in or desist from certain activities that involve the use of their data. The ability to exercise freedom to decide, which the court also referred to as 'control', can be easily compromised in the context of modern data processing: *'The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors.'* Thus, the idea of control that individuals should maintain over their data is the essential argument expressed by the Court (though the Court also clearly stressed that this control might be limited under the principle of proportionality).

The German Constitutional Court's interpretation of the right to self-determination inspired the drafters of the EU Charter. In fact, some see informational self-determination as a main source for Article 8 on the right to data protection.[548] This is not surprising, because informational self-determination and data protection have two corresponding effects. The first is preventing sensitive information from shifting from one context (e.g. the working world, medical treatment, family life, etc.) into other ones, thus creating a sphere in which an individual can feel safe and act free from any interference.[549] This equals informational self-determination in the traditional sense, meaning the right to determine what personal data is disclosed, to whom, and for what purposes it is used.[550] The second effect refers to the broader understanding of informational self-determination as the precondition for citizens' un-biased participation in the political processes of the democratic constitutional state and on the markets.[551] The German Constitutional Court has drawn an explicit link to the threat to free democratic society if informational self-determination is not adequately protected.[552] Democratic deficit can also arise as a result of data controllers' profit-oriented behaviour, which causes strong power asymmetries. As explained in Chapter 2, the world's largest data holders have acquired great powers over data. They have even taken the government's place by exercising a supervisory role over the data economy, where government command has often proved ineffective.[553] These power

[545] Stilman (2015) 15, quoting Westin and Kommers.
[546] Bundesverfassungsgericht, Urteil vom 15.12.1983, BverfgE 65, 1, 41.
[547] English translation of the judgement <https://freiheitsfoo.de/census-act/> accessed 4 June 2018.
[548] Jan Philipp Albrecht, 'Hands Off Our Data!' <https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf> 25.
[549] Hornung and Schnabel (2009) 86.
[550] Simone Fischer-Hübner and others, 'Online Privacy: Towards Informational Self-Determination on the Internet' in Mireille Hildebrandt and others (eds), *Digital Enlightenment Yearbook 2013* (2013) 124.
[551] Hornung and Schnabel (2009) 86.
[552] See II.1.a of the judgement. For the English translation see <https://freiheitsfoo.de/census-act/> accessed 4 June 2018.
[553] Klonick (2018).

asymmetries have led to undesirable consequences such as abuses of individual digital identities,[554] filter bubbles,[555] and fake news.[556] Not only does this influence an individual, it also influences society as a whole. By constraining data controllers' behaviour to fit the legal boundaries, informational self-determination and data protection both protect vital collective goods.

4.3.2. Control over personal data and the right to privacy

As explained in Chapter 3, the EU Charter's Article 7 is a broad provision. It was first conceptualised as 'seclusion' (opacity, or privacy as solitude),[557] before being understood as also encompassing a dimension of 'non-interference' (decisional privacy, or privacy as liberty)[558] and, finally, of individual informational control or empowerment (the ability of an individual to control the terms under which his personal information is acquired and used).[559] This last conceptualisation of the right to privacy has come to the fore in Alan Westin's modern definition of privacy as a claim (or a right) of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,[560] and has often been framed as 'privacy as control'.[561] Some US commentators understood privacy as control as a synonym for a bundle of legal rights of ownership, such as rights of possession, alienability, exclusion of others, commercial ex- exploitation, and so on.[562] From the US, the idea of privacy as control was brought to the EU[563] but was never widely accepted. In the EU, the concept of individual control has been used in two ways: as a definitional aspect of privacy and as an instrumental mechanism to realise valuable outcomes such as autonomy and freedom.[564] However, privacy as control has never been understood as a set of traditional ownership rights, but only as a set of specific rights that concern preserving individual respect and human dignity.[565]

The ECHR and the EU Charter do not mention control as a specific aspect of privacy, but European courts have already shown that their interpretation of privacy extends far enough to capture the notion of control over personal data. For example, before the EU Charter was adopted (pre-2009), the CJEU drew on some aspects of control over personal data in the decisions in the cases *Rundfunk*,[566]

---

[554] On abuse of individual identity see Botsman Rachel, 'Big data meets Big Brother as China moves to rate its citizens' *Wired* (21 October 2018) <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> accessed 4 June 2018.
[555] On filter bubbles see Frederik J Zuiderveen Borgesius and others, 'Should We Worry about Filter Bubbles?' (2016) 5 Internet Policy Review 1.
[556] On fake news see Robyn Caplan, Lauren Hanson and Joan Donovan, 'Moderation After "Fake News"' (2018) <https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf> accessed 4 June 2018.
[557] This perspective implies that too much access to a person interferes with privacy. Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 398. See also De Hert and Gutwirth (2006).
[558] Coming close to what Borgesius calls *'freedom from unreasonable constraints on identity construction'*. Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 126.
[559] 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) 62.
[560] Westin (2015) 5.
[561] Solove (2004) 76.
[562] Ibid., 77.
[563] Nadezhda Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25 Computer Law & Security Review 507.
[564] Koops and others (2016) 38.
[565] Ibid.
[566] C-465/00, *Rundfunk* ECLI:EU:C:2003:294, 20 May 2003.

Satamedia,[567] and *Bavarian Lager.*[568] In *Rundfunk,* the Court considered that an employee's lack of control over flows of her personal data resulted in a violation of the right to privacy.[569]

4.3.3. Control over personal data and the right to data protection

One of the reasons that the German Constitutional Court created the right to informational self-determination by drawing on the personality rights was that there was no other provision in the German Constitution that could help the Court deal with fundamental tensions in relation to data protection. The EU legal order, however, incorporates two such provisions: the right to privacy and the right to personal data protection. The latter in particular is centred around the idea of control over personal data. In fact, the ability of an individual to control the terms under which his personal information is acquired and used is often presented as the hallmark of data protection.[570] The right to personal data protection sets out rules on the mechanisms to process personal data and *empowers* one to take steps – i.e., it is a dynamic kind of protection, which follows data in all its movements.[571] It can be argued that this accentuated control which must be in place regardless of whether the data has been made public or not (i.e. the right to privacy does not apply) is what distinguishes data protection from other fundamental provisions and justifies its individual positioning in the EU Charter.[572] For these reasons, Lynskey attributes to control the role of a normative anchor for personal data protection as a fundamental right.[573] The control aspect of the right seems to be the best-fitting response to tangible and, in particular, intangible harms, such as power asymmetries, powerlessness of data subjects, and even discrimination and manipulation caused by modern data processing. With fully transparent data processing and perfect individual control over behavioural targeting data, the risk of manipulation could be reduced.[574] For example, if e-commerce businesses were required to clearly present information about price discrimination when it worked to a consumer's disadvantage, manipulation with the help of personal data processing could be avoided.[575] In addition, the obligation of data controllers to render the rights of data subjects more effective would adjust the balance of power between data subjects and controllers.[576]

Before the analysis continues, one additional remark is necessary. Traditionally, fundamental rights are 'conceived as liberties', consisting of relatively simple, aspirational statements.[577] Administration of these rights is delegated to contemporary human rights institutions.[578] Fundamental rights that reflect control over data, in particular the right to data protection, differ from that 'right-conceived-as-liberty' approach and should instead be described as a 'right-conceived-as-affordance', i.e. a right granting individuals a possibility to act.[579] Similar to private law entitlements, the strength of the 'right-

[567] C-73/07, *Satakunnan Markkinapörssi and Satamedia* ECLI:EU:C:2008:727, 16 December 2008.
[568] C- 28/08, *Bavarian Lager*, ECLI:EU:C:2010:378, 29 June 2010.
[569] *Supra* n 566, para. 73.
[570] Rouvroy and Poullet (2009) 68.
[571] Rodotà (2009) 79.
[572] Lynskey (2015) 192.
[573] Ibid.
[574] Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 127.
[575] Borgesius and Poort (2017).
[576] Lynskey (2015) 214.
[577] Julie E Cohen, 'Affording Fundamental Rights' (2017) 4 Critical Analysis of Law 3-4.
[578] Ibid.
[579] Ibid.

conceived-as-affordance' is that it empowers individual citizens; the disadvantage is that this right also needs to be invoked by individuals.[580]

4.3.4. Control over personal data and the right to property

Protocol 1 to the ECHR defines property as the 'right to peaceful enjoyment of possessions'.[581] The state is only allowed to take control over personal property under strict conditions. *A contrario*, save for those exceptional situations, the right to property symbolises control exercised by an individual person.

As explained above, property is a general term for rules governing access to and *control* of land and other material resources.[582] All property law regimes have one common idea: the ability to exercise control over a thing. This type of control is characterised by its *erga omnes* effect, meaning that control spreads not only to persons or entities with whom someone contracts (e.g. not only to a buyer of a car), but to everyone in the world (e.g. to a potential thief of the car). However, the actual rigour of control depends on the type of property and/or ownership.[583]

With property rights regarding physical goods, the owner typically has exclusive rights and control over a good; in contrast, this is not the case for intangibles such as data.[584] Property in data challenges traditional concepts of civil law, which since Roman times have attributed property to tangible goods. Roman concepts of *ius utendi, fruendi et abutendi* are the most prominent examples of proprietary entitlements, and frankly, one can hardly imagine them being vested in bits of data.[585] Because of these shortcomings, intellectual property rights are typically suggested as the legal means to establish clear ownership and, consequently, control. For structured databases, a *sui generis* database right was created by the EU database protection directive, which protects the 'substantial investment in either the obtaining, verification or presentation of the contents'.[586]

In principle, personal data is no different than any other data, as it is equally intangible and thus the same argument against vesting property rights in data would apply. However, in the data-driven economy data is viewed as a valuable asset, the new oil, and, consequently, a rivalrous good. For example, new business models on the Internet and social media use the so-called *freemium* pricing strategies, in which users obtain services for free but 'pay' with their personal data, often without their own knowledge.[587] While consumers are not charged for the product, they themselves become a

---

[580] Eric Tjong Tjin Tai, 'The Right to Be Forgotten - Private Law Enforcement' (2017) 8 <https://ssrn.com/abstract=2958145> accessed 4 June 2018.
[581] Protocol 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 1.
[582] Stanford Encyclopedia of Philosophy <https://plato.stanford.edu/entries/property/> accessed 4 June 2018.
[583] For instance, lease is a weaker property right than ownership of a land. However, a 999-year lease may come very close to ownership. Elizabeth Cooke, *Land Law* (Oxford University Press 2012) 4.
[584] Data are an intangible asset, which in many ways match the public good character of information and knowledge, at least with respect to non-rivalry in use. Ingrid Schneider, 'Big Data, IP, Data Ownership and Privacy: Conceptualising a Conundrum' (Presentation at the 10th Annual Conference of the EPIP Association in Glasgow, 2015) <http://www.epip2015.org/big-data-ip-data-ownership-and-privacy-conceptualising-a-conundrum/> accessed 4 June 2016. Like other information-related goods, they can be reproduced and transferred at almost zero marginal costs. OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 195.
[585] William Edward Hearn, *Theory of legal duties and rights* (1883) 186.
[586] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77/20 [1996] 27 March 1996, Article 7(1).
[587] European Commission Staff, 'Online Platforms - Accompanying the Document Communication Communication on Online Platforms and the Digital Single Market' (2016) 33.

product by sharing their data.[588] Furthermore, some recent competition law cases concerning market power related to the availability of users' data are another indication of data commodification occurring in the real world.[589] This explains the relevance of the property discourse on personal data.

If personal data was regulated as property, it would fall under the complete control of individuals, producing *erga omnes* effects. Some have suggested that propertisation of personal data would be a good fit for the current economic situation.[590] Property would give personal data protection an *erga omnes* effect – the legal owner of data would be entitled to control that data regardless of its current location (e.g. somewhere on the premises of a third party). In this way, propertisation would be a response to users' decreasing control in the data economy, which is becoming increasingly difficult to exercise.[591]

However, EU data protection law is at odds with the idea of ultimate control suggested by the advocates of propertisation. The right to data protection is focused on one's personality, not one's property.[592] While it is true that both rights, the right to property and the right to data protection, entail some control, the nature of control vested in the two rights differs. The control in property law is ultimate, i.e. entails the ability to give up the object of property and leave the decisions about it up to a third party. In contrast, the control in data protection law does not extend that far, i.e. some entitlements can never be alienable. This seems to be the right balance. Findings from psychological research suggest that a person, because of her bounded rationality, often inappropriately reacts to data processing threats (or does not react at all). Therefore, some degree of legislative paternalism in the sense of limited control is indispensable. In addition, the view of data protection as a human right takes into account the rights of other actors in society. These are recognized in Article 6 of the GDPR which introduces various legal bases for data processing such as public interest and research objectives.

For the above reasons, it would be difficult to claim that the EU law has adopted or could adopt a property regime. The EU legal system clearly prefers the view of control enabled by the human rights (including the data protection right) paradigm over the view of control enabled by the property paradigm. That being said, the EU data protection legislation does incorporate a few property-like entitlements.[593] For instance, some property features can be seen in the newly established right to data portability, which allows the data subject not only to obtain a copy for his own use, but also 'to transmit those personal data […] into another [processing system], in an electronic format which is commonly used' when the data subject has provided these data.[594]

4.4. Control and EU data protection law

Contrary to the normative conceptualisations of control explored in section 4.3. on fundamental rights, the notion of control becomes more tangible on the level of secondary law, coming closer to what

[588] Tene and Polonetsky (2013) 255.
[589] See section 3.3.4.
[590] Lessig (2006) 228-231.
[591] Ibid.
[592] Rodotà (2009) 81.
[593] Nadezha Purtova, 'Property in Personal Data' (Tilburg University 2011); Jakob M Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 The Yale Law Journal 513.
[594] Purtova (2011) 25.

Black's Law Dictionary describes as a power to direct, manage, oversee, and/or restrict the affairs, business, or assets of a person or entity.[595] Control features can be found in several legal domains: in property law through ownership entitlements, corporate law through the division of roles between owners and managers, consumer protection law through the right to information and withdrawal, and data protection law through (among others) data subject control rights. The latter is of particular interest for this study.

4.4.1. Policy vision for individual control in the data-driven economy

EU policy documents preceding the new EU regulation on personal data suggested that the concept of data subject control most genuinely reflects the contemporary understanding of personal data protection.[596] In 2011, when explaining the blueprint for the future EU regulation on data protection, Vivian Reding pointed to individual control as a central notion in the legal reform: *'I am a firm believer in the necessity of enhancing individuals' control over their own data.'* In her speech, Reding envisioned four pillars of individual control that should form the basis of the upcoming legislation: the right to be forgotten, transparency (information), privacy by default (consent), and protection regardless of data location.[597]

During the legislative process, Reding's ideas were somewhat watered down. For example, after the intense lobbying from some leading business representatives, the right to be forgotten lost its initial strength. Nevertheless, control was preserved in the GDPR's final version as an important underlying idea: *'Natural persons should have control of their own personal data,'* reads Recital 7. Moreover, Reding's pillars idea found its way in the enhanced section on control rights and the updated provision on consent.

During the GDPR adoption process, the notion of control emerged several times in legislative and policy documents of highly diverse natures, ranging from preparatory works for legislation and legislative text, to experts' opinions and vulgarised material addressed to citizens, e.g., in the 2012 Communication from the Commission 'Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century'; in the 2012 European Commission brochure and movie 'Take control of your personal data'; and in the 2010 Communication 'A comprehensive approach on personal data protection in the European Union'.[598] In particular, data subject rights were put forward as a tool at the disposal of the data subjects to enable them to be in control at the different stages of the processing of their data.[599,600]

---

[595] 'control' *Black's Law Dictionary* (1910).

[596] In particular those pertaining to the Regulation, such as the Commission's proposal. *Supra* n 30. Also see European Commission, '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' (2010).

[597] Viviane Reding, 'SPEECH 11/183 Your data, your rights: Safeguarding your privacy in a connected world' (Brussels, 16 March 2011) <http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm> accessed 4 June 2018.

[598] Lazaro and Métayer (2015) 17-18.

[599] Lynskey (2015).

[600] The European Commission was vocal in conveying the idea of control over (personal and non-personal) data in relation to the growing European data economy. In its plans on future regulation of data flows, the Commission discussed how assigning control to a particular entity would contribute to a boost of the data economy. For example, the Commission discussed control in the context of data traceability: *'Traceability and clear identification of data sources are a precondition for real control of data in the market.'* European Commission, 'Communication from the Commission to the EU Parliament,

The Article 29 Working Party discussed control in some of its influential publications. For example, in the opinion on consent from 2011, it held that *'[i]f it is correctly used, consent is a tool giving the data subject control over the processing of his data.'* In the guidelines on the right to data portability, it stressed that *'[t]he purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.'*[601]

The diversity of authorities and documents that have dealt with the concept illustrates the pervasiveness of the rhetoric of control on the EU level.[602] However, this rhetoric was not adopted by the Court of Justice. A brief review of the recent case law indicates no particular intention of the Court to follow the control-oriented policy diction, though this cannot be excluded in the future. It should be kept in mind that some of the CJEU's judgements could be interpreted as arguing for informational control.[603] In addition, the Advocate Generals' opinions, which often pave the way for the CJEU judgements, often draw on the Article 29 Working Party's opinions. Therefore, it is plausible that its views on control could be influential in, for instance, future decisions on data portability.[604]

4.4.2. Reflections of control in the GDPR

As explained in the previous chapter, the GDPR is the EU's key legal act regulating the processing of personal data in the data-driven economy. Control over personal data is reflected in several data protection legal mechanisms, most apparently in the provisions on consent and control rights. Clearly, control is not an exclusive objective of EU data protection law. On the contrary, rules in data protection law are two-fold: they either relate to control over personal data or to protection of personal data. The first group is directed to individuals and enhances their control over data, whereas the second is directed to data holders and imposes a duty on them to protect personal data. In the data-driven economy, actual control over data most often lies in the hands of (big) data controllers. The aim of the law is to limit this control by imposing protection duties and tilting the balance in favour of *individual* control that stems from personal autonomy and other values.

The EU data protection law is thus an inherently binary legislation. However, the control side has recently garnered more attention. The GDPR has strengthened and extended provisions on data subject control and consent. Policy documents and opinions explained above restate the same vision. Interestingly, this policy vision is in strong contrast with the current situation in the data economy. As shown in Chapters 1 and 2, the information outburst has led to a situation in which consumers are inevitably losing control over their data. The divergence between the harsh economic reality and the regulatory utopia makes control-related provisions both highly relevant and potentially controversial.

---

the Council the European Economic and Social Committee and the Committee of the Regions - Building a European Data Economy' (2017) 12.

[601] The Working Party also addressed control in the opinion on the concepts of controller and processor from 2010. However, this is a different type of control than the one discussed in relation to individuals. Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010).

[602] Lazaro and Métayer (2015) 15.

[603] Most apparently, in the Google Spain case (*Google Spain*, C-131/12, ECLI:EU:C:2014:317). Also see the judgement of 7 May 2009, *Rijkeboer* C-553/07, ECLI:EU:C:2009:293, para. 49.

[604] See for example AG Opinion from 24 October 2017 in Wirtschaftsakademie Schleswig-Holstein C-210/16, ECLI:EU:C:2018:57, AG opinion from 12 May 2016 in Breyer C-582/14, ECLI:EU:C:2016:339, AG opinion from 25 June 2015 in Weltimmo, ECLI:EU:C:2015:426, AG opinion from 7 October 2014 in Ryneš, C-230/14, ECLI:EU:C:2014:2072, AG Opinion from 25 June 2013 in Google Spain and Google, C-131/12, ECLI:EU:C:2013:424.

Data protection control-related provisions can be split into two large groups: consent and data control rights.[605] This indicates that individual control should extent to two stages in the data value chain: data collection and secondary uses of data.[606] In the collection stage, consent and the right to information are the key principles. In the second stage, control rights such as the rights to be forgotten, to object, and to access are of particular importance.[607]

Consent pertains to the initial 'yes' or 'no' before data collection starts. However, the role of consent in controlling personal data collection is reduced for two reasons. First, consent does not give control over processing in all cases. If contract, legitimate interest, or public interest are used as a basis for data processing, the reach of consent is curtailed. Second, there is growing scepticism regarding the effectiveness of informed consent in the context of personal data processing, in particular in relation to the requirement for informed consent.[608] Due to the complexity of data processing, being effectively informed has become nearly impossible. Overload of consent-seeking privacy notices has resulted in consent desensitisation.[609] Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when asked to do so.[610]

The GDPR explicitly allows for withdrawal of consent (Article 7(3)), but the option to withdraw faces as many challenges as consent itself.[611] This makes the possibility of extending individual control through data subject consent beyond the data collection stage, i.e. into the secondary use stage, highly theoretical.

Control rights, on the other hand, offer more leeway. These rights apply when processing is based on consent or some other legal basis. This is important in addressing controversial secondary uses of data, which are often based on a contract or legitimate interest. Thus, data subject rights could to some extent work as use regulation (for instance, Article 22's provision on automated decision-making) and thus enable control that extends beyond consent's take-it-or-leave-it approach.[612] Furthermore, having been strengthened by the CJEU's recent interpretation and extended in the updated data protection law, data subject rights seem to somewhat adapt to the new data-driven reality.[613] To summarise, control rights seem to represent a key legal instrument to enhance individual control in the data-driven era. This justifies a detailed analysis of control rights in the following chapters.

4.4.3. Clustering control rights in the GDPR

The EU data protection reform in 2016 introduced an extended section on data subject rights. Under the GDPR regime, the catalogue of control rights consists of the following eight entitlements: the right to information (Articles 14 and 15), the right to access (Article 15), the right to rectification (Article 16),

---

[605] See for example Lynskey (2015); Mantelero (2014); Lazaro and Métayer (2015).
[606] Chapter 2 discussed stages of the data value chain in more detail.
[607] In particular when processing is not based on consent.
[608] Bart Custers, 'Click Here to Consent Forever: Expiry Dates for Informed Consent' (2016) 3 Big Data & Society 2.
[609] Schermer, Custers and van der Hof (2013) 12.
[610] Ibid.
[611] It creates a take-it-or-leave-it situation, assumes that nothing changes during the length of the contract and most users do not seem to cancel their free accounts anyway. Custers (2016) 4.
[612] Joris Van Hoboken, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and Us Frameworks for Personal Data Processing' in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 237.
[613] See for example Brkan (2016).

the right to erasure/to be forgotten (Article 17), the right to restriction of processing (Article 18), the right to data portability (Article 20), the right to object, and the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning an individual or similarly significantly affects her (Articles 21 and 22).

One of the major amendments that the GDPR has brought to the existing data privacy laws is the enhancement of the package of rights of the data subject, strengthening and detailing existing ones, and introducing new ones.[614] This is in line with what was discussed in the previous section about the growing interest of regulators in increasing *'data subject control and empowerment'*. Indeed, the data-driven reality has opened the way to powerful data barons who seem to control our data more intensively (and more subtly) than ever before. Shifting some control towards consumers is a logical reaction.

In comparison to the DPD, the setup of data subject rights in the GDPR is significantly amended. While the directive listed the rights under Article 12 and, somewhat confusingly, grouped them as rights to access, the regulation has taken a much more structured approach. Chapter 2 of the GDPR splits the rights into different groups starting with transparency requirement and the right to information, going on to the rights to access, to erase, and to data portability. Interestingly, the right to information has clearly been made a part of the data subject rights bundle. Moreover, quite significantly, the GDPR now explicitly includes two new rights: the aforementioned right to erase (the right to be forgotten) and the right to data portability.

Drawing on EU statutory and case law, the following chapters provide a detailed analysis of data subject control rights. For the purpose of this analysis, the scope is limited to six rights:

1. The right to information, including the provisions on transparency,
2. The right to access,
3. The right to erasure,
4. The right to data portability,
5. The right to object, and the right not to be subjected to automated individual decision-making.[615]

Each of the following chapters of this thesis (Chapters 5 to 9) refers to one of the points listed above. The selection appears in line with some earlier academic endeavours to organise the rights.[616] As a careful reader may note, some data subject rights (the right to rectification and the right to restriction) are disregarded. As mentioned in Chapter 1, this is not to say that these rights are irrelevant in the light of the big data discussion. The reason for the exclusion is that they share similarities with the right to

[614] Gabriela Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 6 International Data Privacy Law; Daniel Solove, '10 Implications of the New EU General Data Protection Regulation (GDPR)' *Teachprivacy* (23 December 2015) <https://www.teachprivacy.com/new-eu-data-protection-regulation-gdpr/> accessed 4 June 2018.
[615] An alternative way to organise the rights could be a two-fold division into the following two groups: 1. Information and access rights 2. Active rights incl. consent. Lazaro and Métayer (2015) 22-23. See also Dara Hallinan and others, 'PRESCIENT Deliverable 3: Privacy, Data Protection and Ethical Issues in New and Emerging Technologies; Assessing Citizens' Concerns and Knowledge of Stored Personal Data' (2012).
[616] See for instance Gabriela Zanfir, 'Drepturile Persoanei Vizate În Contextul Prelucrării Datelor Private' (University of Craiova 2013).

erasure (Article 17) and the right to object (Article 21). Thus, their limitations and prospects are, to a large extent, reflected in the analysis of the rights in Articles 17 and 21.[617]

4.5. Individual control – a challenging aspiration

The previous section established that individual control represents a central notion in the system of EU data protection law. However, in the data-driven economy, individual control has become a challenging aspiration. Based on the findings in Chapter 2 and in section 4.2., it is possible to identify three types of technological, economic, and psychological causes, all of which are rooted in the specific characteristics of the data-driven economy, that weaken individual control. *Technological* causes refer to the intangible and invisible nature of data-driven technologies, which open up possibilities to duplicate and share data in opaque and less controlled ways than physical goods. In such an environment, it becomes much more difficult to exercise effective control over data. *Economic* causes refer to the market forces that have created a situation in which data barons' dominance over digital information is no longer counter-balanced by control of other actors. Data barons are companies that have access to a large amount of personal data, which makes them increasingly powerful. Data platforms, operating on a two-sided market, are a typical example.[618] To enrich data that is provided or generated by users, platforms acquire additional personal data by collaborating with data brokers or using open source data. Later, they recoup their investments by reusing the data or by sharing it with multiple parties.[619] This sort of data reuse is problematic because it is opaque, technologically complex, [620] and therefore fundamentally challenges the idea of individual control. Finally, *psychological* causes often prevent individuals from exercising effective control over data. Data subjects lack the ability and motivation to scrutinise key details of personal data processing necessary to make informed decisions about their data.[621] The phenomenon of 'bounded rationality' adds to the problem. Individuals' judgements and decisions are often not reached on the basis of a rational optimisation process, but are instead the result of heuristic and biased information processing.[622]

4.6. Conclusions

By exploring the concept of control, this chapter answered the third research sub-question regarding the notion of individual control and its relation with data subject rights. While doing so, it established a bridge between the general overview of the data-driven economy and the pertaining legal framework, and the specific analysis of data subject control rights.

---

[617] That said, the rights may evolve into a more significant provision in the future. This will depend on the further guidance regarding the articles' scope of application. See Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2017) 2 Journal of Information Rights, Policy and Practice.

[618] Chapter 2, section 2.3.1.

[619] Will Oremus, 'The Real Scandal Isn't What Cambridge Analytica Did' *Slate.com* (March 20, 2018) <https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html> accessed 22 May 2018.

[620] They also exceed regulatory expectations and supervisory powers. Pasquale (2015) 2.

[621] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016, 19.

[622] Gigerenzer and Reinhard Selten, *Bounded Rationality: The Adaptive Toolbox* (MIT Press 2002).

Individual control represents a central notion in philosophical discussions related to people's autonomy and freedom. Lack of effective control translates into deterioration of some essential values. In psychology, control represents an essential condition for individual well-being.

Individual control over data plays a role in the provisions of primary and secondary EU law. On the primary law level, control is integrated in several fundamental rights. In the context of this study, the right to data protection stands out as its 'control' aspect links directly to data subject rights.

Among the secondary law sources, the notion of control stands out in data protection law. The analysis of the provisions in the latter reveals two facets of control: the first is normative, meaning that control links back to the values that underpin the entire legal field, while the second is instrumental and materialises through the provisions on data subject rights. This second facet is what the remaining chapters focus on.

In spite of being a central notion in data protection law, the notion of individual control undoubtedly faces many challenges. In particular, technological, economic, and psychological causes, all of which are rooted in the specific characteristics of the data-driven economy, weaken individual control. The remaining chapters will analyse to what extent data subject rights are resistant to these challenges or, in other words, how effectively these rights afford control to data subjects.

5. THE RIGHT TO INFORMATION

5.1. Introduction

This chapter addresses the right to information, the cornerstone of the system of control rights under the GDPR. In the EU DPD, the right to information was separated from the rest of the provisions on data subject rights. However, the GDPR altered the directive's structure and made the right to information a constituent part of Chapter 3 (data subject rights).

The right to information is *primus inter pares* among the data subject rights. Formally, all the rights are deemed equal, but in practice the right to information stands out as it exemplifies the principle of transparency and represents the focal point for all other data subject rights. Without the necessary information, a data subject cannot meaningfully participate in the data economy, nor can she exercise her other control rights.[623] The story of Max Schrems is telling. Schrems, who became famous after having sued Facebook for not complying with EU privacy laws, used the right to information and access to go after the social media giant.[624] If Schrems had had no knowledge about the amount and quality of data which Facebook had processed about him, he would have had difficulty disagreeing with its data processing practices in first place. This view finds support in the CJEU's ruling in *Bara*: *'The right to information is the precondition for other rights: the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed […] and their right to object to the processing of those data […].'*[625]

By exploring the GDPR provisions on the right to information and the corresponding parts of the ePrivacy directive,[626] this chapter seeks to answer the fourth research question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* While this research question refers to data subject rights as a whole, in this chapter the scope is narrowed down to what is necessary to understand the right to information, and to assess the vigour of control that it offers to individuals.

This chapter starts with a brief discussion of the normative bases of the right to information in section 5.2. Section 5.3. then turns to three aspects of the right: the content, the format, and the timing required to convey the necessary information. Special attention is given to the right to explanation of automated decision-making, which is to some extent a novel concept. In addition to the GDPR's provisions on the right to information, ePrivacy law contains some specific rules on the right to information in the electronic communications sector. These are explained in section 5.4. Throughout

---

[623] Max Schrems received knowledge about Facebook's data processing when he was studying in the US and listening to a lecture by a Facebook privacy counsel. Helena Ursic, 'How a study exchange triggered a CJEU landmark case' (*Leiden Law Blog,* 20 October 2015) <http://leidenlawblog.nl/articles/how-a-study-exchange-triggered-a-cjeu-landmark-decision> accessed 5 June 2018.

[624] Cyrus Farivar, 'How one law student is making Facebook get serious about privacy' *ArsTechnica* (15 November 2012, <https://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/2/> accessed 5 June 2018.

[625] C-201/14 *Bara and Others* [2015] ECLI:EU:C:2015:638. Also see the Opinion of AG Cruz Villalón in the same case.

[626] I analyse both the currently valid ePrivacy Directive and the proposed ePrivacy Regulation. The focus is on the directive. When I refer to the regulation, I will mention it specifically.

the chapter, the positive and negative implications of the data-driven economy for the right to information are carefully considered. Based on the findings, section 5.5. provides an answer to the control-related research sub-question.

5.2. The link to fundamental values

The GDPR's version of the right to information stems from some fundamental values: privacy, autonomy, transparency, and fairness.

The right to information is particularly strongly intertwined with transparency as a fundamental value. In both the private and the public sector, transparency serves the objectives of legitimate governance. More transparency regarding the decisions of a decision-making body, either of the government or of a powerful company, encompasses equality or, in other words, the *balance of powers*.[627] Considering strong information asymmetries in relation to personal data processing on the data-driven markets,[628] it quickly becomes clear why the ideas behind transparency and other human rights must apply equally to private sector actors.[629]

As Chapter 2 showed, complex data flows and automated (i.e. algorithmic) decision-making have become standard elements within the data-driven value chain. In the banking,[630] health-care,[631] automotive,[632] and even agricultural sectors,[633] a great many decisions and processes are driven by data mining and influenced by AI. These trends unavoidably lead to less transparency and more information asymmetries. Algorithms often act as black boxes, not allowing for data subjects' supervision, understanding, or any other aspect of control.[634] Worse still, deficiencies in the quality and

[627] See Chapter 2, section 2.4.2.4.

[628] Information asymmetries between the companies, regulators and consumers came to light during the hearing of Mark Zuckerberg in the US Congress on April 10, 2018, where some of the congressmen revealed fundamental flaws in their understanding of the data economy. Transcript of the hearing of Mark Zuckerberg in the US Congress on April 10, 2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.013eea956ff1> accessed 28 May 2018.

[629] Sophie van Bijsterveld, 'A Crucial Link in Shaping the New Social Contract between the Citizen and the EU' in PJ Stolk and others (eds), *Transparency in Europe II: Public Access to Documents in the EU and its Member States* (Ministry of the Interior and Kingdom Relations Constitutional 2004) 65. The Facebook/Cambridge Analytica scandal is a telling example why transparency is important to guaranteeing legitimate governance of private sector entities. If the Guardian had not revealed Facebook's failure to stop unauthorized data mining, no one would have known about political manipulation on Facebook preceding the US elections and Brexit campaigns. In the future, Facebook plans to label political ads as "sponsored" to enhance transparency of the posters. Carole Cadwalladr and Emma Graham-Harrison, 'How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool' *The Guardian* (17 March 2018) <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> accessed 5 June 2018.

[630] For example, to early detect credit card fraudulent activity.

[631] For example, to conduct graphical analysis and comparison of symptoms.

[632] For example, to analyse drivers' patterns to improve the technology.

[633] Liliya Pullmann and others, 'WP3 Test of the Model; D3.2 Test Report (Deliverable for the EuDEco H2020 Project)' (2017) <http://data-reuse.eu/wp-content/uploads/2017/09/Test-report-final.pdf> accessed 5 June 2018.

[634] COMPASS, a tool to predict the probability of recidivism used in US courts, was deemed fair by its manufacturer (Northpointe) according to one metric, but found unfair in a later study by ProPublica according to another metric: *'… in the end the decision which notion of fairness to implement is highly political, especially if the decision making system is applied in societally sensitive contexts. Society needs to be made aware of this more.'* Jaap-Henk Hoepman, *'Summary of the CPDP panel on algorithmic transparency' (Blog XOT,* 26 January 2017) <https://blog.xot.nl/2017/01/26/summary-of-the-cpdp-panel-on-algorithmic-transparency/> accessed 5 June 2018.

quantity of the data available to train and test them may lead to discrimination and biases that are always hidden from the public eye.[635]

For these reasons, the need for transparency remains pressing in the data-driven economy. Achieving 'transparent processing', however, is not an easy task and requires more than just information disclosure.[636] In the big data context in particular, providing information must be done *fairly*, that is with particular consideration for an individual's needs. The fact that an individual is probably the weakest link in the data economy draws an important analogy to consumer regulations. In fact, it has been argued that the fairness test in the unfair terms directive[637] could be used to give substance to the notion of fairness in the GDPR.[638] Specifically, fairness could be assessed based on two components: 'good faith' of the data controller and 'significant imbalance' between the controller and the data subject.

5.3. Regulatory framework under the GDPR

5.3.1. The content of the communicated information

5.3.1.1. The information catalogue

Articles 13 and 14 of the GDPR represent the core of the right to information. These two provisions provide a detailed catalogue of the facts to be communicated to a data subject as part of her right to information. The binary nature of the provisions suggests that two types of situations must be distinguished: 1) when data is obtained directly from the data subject, and 2) when data is obtained from third parties.

A typical example of the first situation is the collection of information from a user of a social media network. The moment he signs up for the service and his personal data is about to be processed, the data controller must provide this user with the set of information listed in Article 13.[639] To illustrate the second situation, we can think of a hiring manager within a large enterprise who tries to identify suitable candidates by using information available on social media. Also in this second case, candidates have to be informed about data processing – for example in the job ad.[640] When data is not obtained

[635] Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 California law review 671, 693.
[636] A strong link is established in Recital 60 of the GDPR: "*The principle of transparency requires […] any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.*" Section 5.3.2. analysed the exact meaning of that phrase.
[637] *Supra* n 499.
[638] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness Data Protection and the Role of Fairness' [2017] CiTiP Working Paper Series 33-34. Also see Helberger, Borgesius and Reyna (2017).
[639] According to that article, data subjects should at the minimum receive the information about the identity and the contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the legitimate interests pursued by the controller or by a third party (if this is the legal basis used by the controller), the recipients or categories of recipients of the personal data and where applicable, the fact that the controller intends to transfer personal data to a third country or international organization.
[640] Article 29 Working Party, 'Opinion 2/2017 on Data Processing at Work' (2017) 11.

directly from a data subject, two entities may be held responsible for ensuring the information arrives to the addressees, since they are both controllers of data.[641]

The scope of information that has to be provided to data subjects slightly varies between the two situations. Most apparently, it is only when data is not collected from a data subject that there is an obligation to describe categories of data, e.g. address, gender, behavioural data (Article 14(1)(d)). This is probably because in such cases, the data subject does not have a good overview of/control over the data that is being shared. Describing categories helps her understand the nature and scope of data processing, which might otherwise remain hidden. Furthermore, when data **is not** collected from a data subject but is instead gathered from other sources, a data controller has to provide information about *these sources of data* and, if applicable, whether the data came from publicly accessible sources (Article 14(2)(f)).

The information that provision of data is a *statutory or contractual requirement* is only necessary in situations when data is collected directly from a data subject. This is because a data subject has to know about the reasons behind the request for data: is the request just the commercial strategy of a data controller or are there other reasons behind it? Naturally, the situation fundamentally changes if a *law* requires one to disclose personal information. Moreover, a description of a controller's *legitimate interest*[642] should be part of the standard information catalogue when data is collected from the data subject but not when it is collected from third parties, unless necessary for transparency and fairness of data processing. It is difficult to understand why information about legitimate interests of data controllers is less relevant when data is not obtained from an individual.

It is interesting to note that the original proposal of the GDPR drafted by the Commission did not distinguish between the two situations as Articles 13 and 14 in the current version do. Instead, it combined them in one single article. While there were still some differences depending on whether data was obtained from an individual or not,[643] the idea behind the integrated provision was that the two situations were comparable and that the information duty should be considered holistically. However, in the final version of the GDPR, the idea of a uniform article on the right to information was struck down and the Council returned to the old dichotomy system, as it existed in the DPD. As indicated above, the reasons for differentiating the two situations are not very persuasive. Instead of distinguishing between the situations based on a data subject's contact with a controller, the concern should be the context in which the information is obtained.

---

[641] This is the solution that was mentioned in AG Cruz Villalón's opinion to Bara judgement (C-201/14 *Bara and Others* [2015] ECLI:EU:C:2015:638), para. 39.

[642] Recitals 47-50 of the GDPR give some examples of legitimate interests: processing for direct marketing purposes or preventing fraud, transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data, processing for the purposes of ensuring network and information security and reporting possible criminal acts or threats to public security to a competent authority. In *Rigas*, the CJEU provides a three-step tests to assess legitimate interest – *"first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence."* Case C-13/16 *Rigas* [2017] ECLI:EU:C:2017:336, para 28.

[643] See for more details 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) 1 final.

The GDPR's information catalogue is extensive; this has two consequences. On the one hand, extensive communications impose a burden on individuals who have to digest long and perplexing policies.[644] On the other hand, data subjects gain access to thorough and detailed information. This may be of special importance in the context of the data-driven economy, where people usually have a greatly limited understanding of what actually happens with their data. Five pieces in the GDPR information catalogue are of particular interest as they either carry special significance for individuals' protection in the era of big data or they are novel. By 'carrying special significance', it is meant that the provisions aim to address specifics of the big data economy, for instance frequent changes of the context in which data is processed and the increased use of automated decision-making. The selected elements relate to information about legal bases for personal data processing, storage of personal data, recipients of personal data and third parties, and personal data processing for new (other) purposes. The provisions in Articles 13(2)f and 14(2)g on the information about automated decision-making merit special attention and are analysed in more detail in section 5.3.1.2.

5.3.1.1.1. Information about legal bases

Contrary to the DPD, which did not address this point, the GDPR places emphasis on ensuring that data subjects are aware of the legal basis used to justify the data processing. In the GDPR, conveying the information about legal bases is a mandatory provision (Articles 13(1)(c) and 14(1)(c)). Data controllers are obliged to inform data subjects about any legal bases that they use, for example data subjects' consent, public interest, or a contract between the controller and data subject. If data processing is based on a legitimate interest of a data controller, these interests also have to be elaborated and communicated to a data subject (Articles 13(1)(d) and 14(2)(b)). By receiving the information on legitimate interests, data subjects become more aware of controllers' intentions and can more easily assess what is happening with their data.

The information on the basis of Articles 13(1)(c) and 14(1)(c) should also reflect the results of the balancing test, which controllers are obliged to carry out whenever legitimate interest is used as a basis of data processing. It should be demonstrated that controllers have carefully balanced their commercial interests with the fundamental rights and interests of data subjects, ensuring that their fundamental rights protection is not at risk.[645] This is important because in the case of secondary data uses, controllers are often pursuing solely commercial interests. In such cases, controllers may find it difficult to justify *'in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.'*[646] It is most

[644] Suzanne Rodway, 'Just How Fair Will Processing Notices Need to Be under the GDPR?' (2016) 16 Data Protection - A Practical Guide to UK and EU Law. Also see sections 2.4.2.2. and 4.2.3.

[645] Article 29 Working Party uses the example of pizza order to illustrate when processing cannot be based on legitimate interest. In the example, Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home. Claudia's address and credit card details but also her recent order history (for the past three years) are stored by the pizza chain. In addition, the purchase history is combined with data from the supermarket where Claudia does her shopping online, which is operated by the same company as the one running the pizza chain. Article 29 Working part considers that in such a case a company could not base data processing on their legitimate interests (i.e. pizza delivery and charging for the costs) because they too strongly interfered with Claudia's rights (i.e. collected too much of her personal data). Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' 31.

[646] Ibid., 43.

likely in such cases that the interests of data subjects will prevail over controllers' commercial interests.[647]

The provisions in Articles 13(1)(c) and 14(1)(c) face two challenges. First, they are difficult to implement because they both require a highly specific description of the interests and careful balancing with the rights of individuals. To justify that/why their interests override the rights of data subjects, controllers have to carefully identify and specify these interests in the first place. Furthermore, coming up with a balancing scheme may impose some additional administrative burden.[648] Second, the provisions may be used as a *carte blanche* in a wide range of cases. To avoid generalisation, the balancing test under legitimate interest requires a context-specific assessment and implementation of potential mitigations as part of organisational accountability.[649]

5.3.1.1.2. Information about the length of the storage period

As a new part of the information catalogue, the GDPR obliges data controllers to provide information about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Articles 13(2)(a) and 14(2)(a)). This 'new' category is in line with the principle of storage limitation, which is expressly laid down in the GDPR.[650]

In the data-driven economy, local data storage on external hard drives has almost disappeared. Due to the possibility of limiting cost, companies are increasingly using cloud storage solutions. This has at least two consequences. First, the cost of data storage has decreased; a larger amount of data can be stored for a longer period of time. Second, this new type of data storage typically requires the involvement of a third party in the data processing. Dropbox and Amazon Web Services are two widely known cloud providers commonly used by businesses.

The processing of personal data should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.[651] In particular, this requires ensuring that the period for which the personal data are stored is limited to a strict minimum.[652] This in turn decreases the risk of wrongful or extensive uses, as less data is exposed to potential abuses for a shorter time period. This requirement bears special value given that illegitimate retention of personal information has been among the most significantly contested online information practices.[653] For example, a cloud-based storage provider does not let users' data lie dormant on the servers but often shares or sells it to third parties. Dropbox's privacy policy informs users that the company will not sell their data to advertisers or other third parties.[654] However, it also provides a long list of exceptions, such as government, other

[647] Santos and others, 26.
[648] For an example of such scheme see Centre for Information Policy Leadership (2017), 18. This report gives a surprisingly positive assessment of the possibility to rely more often on legitimate interest as a basis for data processing.
[649] E.g., pseudonymisation of data. Ibid., 29.
[650] Article 5(1)e of the GDPR.
[651] Ibid.
[652] Recital 39 of the GDPR
[653] Joel Reidenberg and others, 'Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding' (2015) 30 Berkeley Technology Law Journal 56. Also in relation to concerns of excessive data retention see Alexander Tsesis, 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data' (2014) 49 Wake Forest Law Review 433 <http://wakeforestlawreview.com>.
[654] Dropbox's privacy policy <https://www.dropbox.com/privacy> accessed 5 June 2018.

users, trusted parties, and other applications.[655] Having the information about data controllers' storage policy also raises awareness of potential data reuses and helps assess their risk.

5.3.1.1.3. Information about third parties and recipients of data

As was shown in Chapter 2, data disclosures and sharing (aimed at combining and reusing third parties' data sources) have become an inherent part of the modern data economy. The negative side of this is that individuals are often unaware of flows and secondary uses of data which do not meet their privacy expectations.[656] The requirement in Articles 14(1)(e) and 13(1)(e) seems to have acknowledged this struggle. The articles require that controllers provide information about recipients or categories of recipients of personal data.[657] However, the provision is far from the ideal situation depicted in an earlier opinion by the Article 29 Working Party. Namely, the Working Party suggested that when data was collected online, the websites (i.e., controllers) should provide information not only about to whom personal data would be disclosed, but also about *why*.[658] This is not expressly stipulated in the GDPR.

A 'recipient' stands for a natural or legal person, public authority, agency, or other body to which the personal data is disclosed, whether a third party or not. However, the GDPR stipulates that public authorities, which may receive personal data in the framework of a particular inquiry in accordance with EU or member state law, shall not be regarded as recipients (Article 4(9) of the GDPR). This means that the fact that users' data has been shared with public authorities should not be provided under the right to information.

Does this also mean that informing data subjects that their data has been shared with public authorities in the sense of a 'canary clause' is not provisioned/allowed? A canary clause is a statement on a website declaring that the service provider has not received any secret data snooping requests from the government or law enforcement agencies. After such a request has been made, the notice is removed from the website.[659]

It is clear that sometimes protection of public interest and security require absolute confidentiality.[660] However, more transparency over data flows between the government and private data holders seems to be increasingly needed. These flows are ubiquitous, but they are often completely hidden. This issue was also challenged in the PNR case, where the CJEU stressed the importance of transparency regarding data flows to government agencies.[661]

---

[655] Ibid.

[656] See for example the transcript of the hearing of Mark Zuckerberg in the US Congress on April 10, 2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.013eea956ff1> accessed 28 May 2018. Even some of the US Congressmen and Congresswomen were clearly unaware of Facebook's business model and the use of data on the platform.

[657] Differently from the directive, under which this information was only exceptionally provided as part of "further information". See Article 10(c) of the DPD.

[658] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) 31.

[659] 'What is a warrant canary?' *BBC* (5 April 2016) <http://www.bbc.com/news/technology-35969735> accessed 5 June 2018.

[660] See article 23(1) which lists exceptions to data subject rights.

[661] Opinion 1/15 of the Court regarding Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data [2017] ECLI:EU:C:2017:592, para 223.

Interestingly, the EU Parliament's (LIBE) proposal for the GDPR contained a requirement to inform a data subject '*whether personal data was provided to public authorities during the last consecutive 12-month period*'.[662] The provision was later removed from the information requirement.[663] This removal does not suggest that a canary clause or some general information on data sharing with the government should not be presented to data subjects at all. On the contrary, a general clause can be a helpful tool to achieve more transparency about data flows (while not jeopardising ongoing investigations).[664]

The provision requiring that information about recipients always be provided to data subjects is of course a welcome improvement. It is, however, limited by the scope of the GDPR. For instance, once data is anonymised, data protection law in principle ceases to apply.[665] In the case of anonymised data sharing, recipients do not have to be disclosed.[666]

5.3.1.1.4. Information about new (other) purposes of data processing

Where a controller intends to further process personal data for a purpose other than that for which it was collected, prior to that further processing the controller shall provide the data subject with information on that other purpose and any further relevant information (Articles 13(3) and 14(4)).[667]

In practical terms, this obligation means that if the controller later processes personal data for a new purpose not covered by the initial notice, then it must provide an updated notice covering this new processing.[668] This requirement did not exist in the DPD. It is yet another reflection of the changes that have taken place in the global economy in recent years and to which the legislator paid special attention. Data reuse and sharing have been two of the key business strategies of data-driven companies. A typical example is social media platforms: data collected by users is traded to third parties, e.g. advertisers or data brokers, to be reused for their specific purposes.[669] Furthermore, predictive analysis may transform information about someone's shopping habits into information on someone's health status (e.g. pregnancy). In the well-known Target case, a store learned that a

---

[662] European Parliament, 'European Parliament, 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)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))' Committee on Civil Liberties, Justice and Home Affairs (LIBE)(2013) Amendment 110 <http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf> accessed 5 June 2018.

[663] The reasons are unknown. My assumption is that the security objectives prevailed over the need for transparency.

[664] Some data controllers already provide such information, see for example Facebook's privacy policy and their transparency report <https://transparency.facebook.com/government-data-requests> accessed 5 June 2018.

[665] However, this depends on the strength of anonymisation. It is possible that anonymised data is de-identified. Then data protection law would apply again. See for example Tene and Polonetsky (2013) 257.

[666] The case of Unroll, a free inbox cleaning software, well illustrates issues at stake. ' *... while Unroll.me is cleaning up users' inboxes, it's also rifling through their trash. When Slice found digital ride receipts from Lyft in some users' accounts, it sold the data off to Lyft's ride-hailing rival, Uber.'* Amanda Hess, 'How Privacy Became a Commodity for the Rich and Powerful' *The New York Times* (May 9, 2017) <https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html> accessed 5 June 2018.

[667] Article 13 (3) of the GDPR.

[668] Bird & Bird (2017) 21.

[669] The lack of vocabulary complicates the definition of the phenomenon of 'online personal data trading'. Advertisers pay to social networks to place relevant ads. The ads are allocated to a user based their profiles. Although, formally speaking, the advertisers *pay for a service* to Facebook, what actually happens is a sale of consumers' data. However, the social media executives vehemently refuse to frame this as 'selling of data'. See for instance the exchange between Mark Zuckerberg and senators at the hearing in US Congress on April 10, 2018, *supra* n 628.

teenager was pregnant before her father did. Based on the teenager's shopping profile, which was comparable to that of pregnant women in its database, the retail store predicted that she was expecting a baby and started sending advertisements for maternity products. This became a huge scandal after the teenager's father (and not the teenager herself) received the ads. The story clearly demonstrates the unexpected and out-of-context insights that predictive analysis may have.

Changes to the purpose of data processing often happen as part of a business routine. Recruiters use social media data to pre-screen suitable candidates. This challenges the privacy expectations of social media users. Most people who share personal data on social media expect it to be processed for the purpose of enabling online communication and find it surprising when this data is processed as part of a recruitment strategy. Without receiving specific, preliminary information about intended purposes, it is extremely difficult for any individual to ascertain to which uses specific data is actually being put.[670] Conveying information about the purposes is even more important as data reuse is increasingly carried out behind the scenes.

As mentioned in the overview of the EU data protection law in Chapter 3, purpose limitation is one of the core restrictions in this law. Under the principle of purpose limitation, data cannot be reused unless the controller ensures a valid legal basis for this secondary use, e.g. a data subject's additional consent. This is of course at odds with the big data business practices, which tend to make a profit from data secondary uses. Furthermore, the process might become lengthy and inefficient if each time a data controller uses the data for a new purpose, this has to be communicated to data subjects. Yet, the GDPR remains strict in this regard, as do some EU data protection authorities. In a letter to Microsoft regarding its Windows 10 privacy policy, the Article 29 Working Party expressed concerns about the scope of data being collected and further processed.[671] Microsoft processed data collected through Windows 10 for different purposes, including personalised advertising. It appears from the letter that this general description was not enough for the EU watchdog: '*Microsoft should clearly explain what kinds of personal data are processed for what purposes*,' the Working Party wrote, demanding Microsoft's immediate reaction.[672] Moreover, a recent document of the Dutch DPA confirms that authorities are dedicated to keeping the principle intact. The DPA found that Facebook acted in breach of data protection law as the company did not adequately inform data subjects that *'it can track web surfing behavior and app usage outside of Facebook and use these data for advertising purposes.'*[673] This sort of tracking may easily cross the boundaries of purpose limitation, but it is difficult to notice

[670] In a 2015 report, KU Leuven researchers point at Facebook's DUP which only provides a broad overview of the purposes for which it processes personal data. '*This overview, however, is extremely generic and encompasses all data collected by Facebook*.' Alsenoy and others (2015) 66.

[671] Letter of the Working Party 29 to Microsoft from 12 January 2016 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi5tPrJoJPVAhVB9IMKHeg0Bv8QFggoMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D42572&usg=AFQjCNHHyjIqeD5bRZFDbiXGX2rEwlfVQA> accessed 5 June 2018.

[672] Ibid.

[673] Informal English translation of the conclusions of the Dutch Data Protection Authority in its final report of findings about its investigation into the processing of personal data by the Facebook group from 23 February 2017 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_facebook_february_23_2017.pdf> accessed 5 June 2018.

and escape from. Direct information – the Dutch DPA stressed the need to provide information in the first layer of the privacy notice – is therefore of paramount importance.[674]

5.3.1.1.5. Information about the sources of data

When data is obtained from third parties, controllers have an additional duty to provide information about those third-party sources and, if applicable, whether the data came from publicly accessible sources (Article 14(2)(f)). This is another novel provision in the GDPR that also seems to fit new circumstances in the data-driven economy, where data collection is rarely limited to one source.

For example, consider the new trend in the pharmaceutical industry: real world data (RWD). RWD is used to improve clinical trials with data collected from sources outside the traditional clinical environment. These sources may include large simple trials, pragmatic clinical trials, prospective observational or registry studies, retrospective database studies, case reports, administrative and health-care claims, electronic health records, data obtained as part of a public health investigation or routine public health surveillance, and registries (e.g., device, procedural, or disease registries).[675] The unique combination of sources can contribute to better results of clinical trials and enable more precise analysis of drugs' effects. However, by connecting different sources, it is easy to reveal facts about a person and infringe her privacy. A combination of someone's social media profile and her clinical trial report can be much more insightful and, for precisely these reasons, privacy-infringing. Combining data sources is also a trend on some other data-driven markets. Facebook has admitted to regularly combining and enriching its own data with databases purchased from Acxiom.[676] Merging someone's social media profile data with information about his health or race can be a valuable source of information for advertising companies – those that are Facebook's most loyal clients.[677] In a recent opinion, the Dutch DPA pointed to the lack of transparency in relation to Facebook's data sources, which also added to the violation of its information duty: '*The Facebook group does not offer a central overview of the personal data it processes for advertising purposes since the change of the privacy policy. The information is scattered over different sources. Because of this, data subjects do not receive a clear and understandable overview of the data processing with the highest impact on their private life in the first information layer.'*

The two examples above illustrate why knowing about sources is critical to be aware of the scope of data processing. However, the GDPR's rule to disclose sources has been watered down by the guidelines in Recital 61. Namely, if the origin of the personal data cannot be provided to the data subject because various sources have been used, the recital suggests that only general information

---

[674] *'The Facebook group is able to do this as soon as a Facebook user visits a website or uses an app that contains a Facebook 'like' button, or other interaction with Facebook, even if the user does not click on that button, and even if the user has been logged-out of the service.'* Ibid.

[675] Food and Drug Administration, 'Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices - Guidance for Industry and Food and Drug Administration Staff Document' (31 August 2017) <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm513027.pdf> accessed 23 September 2018.

[676] Only recently, under the media and public pressure, they abandoned this practice. Drew Harwell, 'Facebook, longtime friend of data brokers becomes their stiffest competition' *The Washington Post* (29 March 2018).

[677] Jim Edwards, 'Facebook's Big Data Partner Knows Who You Are Even When You Use A Different Name On The Web' *Business Insider* (September 26, 2013) <http://www.businessinsider.com/facebook-and-acxioms-big-data-partnership-2013-9> accessed 5 June 2018.

should be provided. This provision appeared in the GDPR text after the Council's intervention and allows for a wide interpretation of how far information duty under Article 14(1)(f) actually extends.[678]

In the technical terminology, the discussion on data sources has been framed as data lineage or provenance: a description of where data came from, how it was derived, and how it is updated over time.[679] One important reason to be interested in data lineage is to find sources of errors. Thus, controlling the truthfulness of the data is at the heart of data lineage. The GDPR requirements on data sources convey a similar idea. By transparently presenting the sources, it is more likely to control data's adequate use and outcomes of its analysis.

5.3.1.2. The right to explanation

5.3.1.2.1. Information about automated decision-making in Articles 13 and 14

Another highlight in Articles 13 and 14 is the right to receive information about automated decision-making. At least when data controllers engage in automated decision-making, including profiling, which is based solely on automated processing and which produces legal effects concerning a data subject or similarly significantly affects a data subject,[680] data subjects must be provided with meaningful information about the logic involved in the decision-making and about its significance and envisaged consequences (Articles 13(2)f and 14(2)g).

In the DPD, information about the logic behind automated decisions was only provided if a data subject herself demanded so through her right of access (Article 12a of the DPD). The GDPR has preserved this provision but also includes information on automated decision-making in the standard information catalogue.

This new information duty has sometimes been referred to as a right to *explanation*, suggesting that it could work as a right to clarification of complex algorithms and decisions inferred from them.[681] In the context of the data-driven economy, the right to explanation could indeed play an important role. Data-driven decisions are often hidden from the public eye, are based on complex algorithms that are difficult to comprehend, and have consequences that cannot easily be predicted.[682] Explanation tailored to the needs of data subjects thus appears to be desirable.

The duty to provide information on automated decisions is not limited to the cases where the decisions produce legal effects; these are only the cases where informing data subjects is *mandatory*. However, given the risks of automated decision-making, it could be argued that the right should have a broader scope. Automated decision-making, in particular profiling, often lead to discrimination and causes

---

[678] Materials from the GDPR negotiations in the Council <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.

[679] Leonardo Haut, Marius Brinkmann and Sven Abels, 'WP2 Developing the Initial Model: D2 .4 Report on the Technological Analysis (Deliverable for the Eudeco H2020 Project)' (2016) 7 <http://data-reuse.eu/wp-content/uploads/2016/06/D2.4_ReportOnTheTechnologicalAnalysis-v1_2016-02-29.pdf> accessed 5 June 2018.

[680] As for the specific definition of these automated decisions Articles 13 and 14 refer to Article 22 of the GDPR.

[681] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and A "right to Explanation"' <http://arxiv.org/abs/1606.08813> accessed 5 June 2018; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2018) 7 International Data Privacy Law 233.

[682] Illustrative is the example of the teachers' ratings used in the US, where the parameters which a teacher is judged upon, are largely unknown. See more in Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).

biases due to deficiencies in the quality and quantity of the data available to train and test the algorithm, as well as problems with data sources and labelling.[683] The risk for fairness is thus inherently present,[684] which is an argument for why information on automated decision-making should almost always be provided to a data subject.

What specifically should information on automated decision-making entail? Based on Articles 13(2)f and 14(2)g, data subjects should receive the following three subcategories of information:

1. Meaningful information about the logic involved in the automated decision-making;
2. Meaningful information about the significance of the processing;
3. Meaningful information about the envisaged consequences of the processing.

Logic stands for the types of data and features considered in an automated decision-making system, and categories in the decision trees used to make a decision.[685] Linear models, which can only represent simple relationships, are typically easy to explain, whereas nonparametric methods such as support vector machines and Gaussian processes, which can represent a rich class of functions, are often highly difficult to interpret.[686] For example, data mining software performing on the basis of multiple variables (even thousands) can lead to a process that is not explainable in human language.[687] It would be difficult for the user of the software to provide a detailed answer to why an individual was singled out to receive differentiated treatment by an automated recommendation system. This is why some have argued that '*algorithmic approaches are alone in the spectrum in their lack of interpretability*'.[688]

Edwards and Veale examined the computer science literature to determine what it means to explain an algorithm in a meaningful way.[689] They identified two types of explanation: subject- and system-centric. The former, which is restricted to the region surrounding a set of data, was suggested as more meaningful, mostly because it enables users 'to build more effective and relevant mental models'.[690] Other solutions that could help convey the logic of the systems to individuals without going into technical details are the use of counterfactuals, simple 'if-then' statements indicating which external facts could be different to arrive at a desired outcome,[691] and case-based approaches that provide explanation by retrieving the most similar cases from computer memory.[692] Finally, a useful explanation of the logic that is used to arrive at the decision should also include an explanation of the type of data on which the decision is based.[693]

---

[683] Dimitra Kamarinou and others, 'Machine Learning with Personal Data Machine Learning with Personal Data' [2016] Queen Mary School of Law Legal Studies Research Paper No. 247/2016.
[684] Among others, power imbalance and violations of the principle of good faith.
[685] Wachter, Mittelstadt and Floridi (2017) 6.
[686] Goodman and Flaxman (2016) 6.
[687] Andrejevic and Gates (2014) 186.
[688] PJG Lisboa, 'Interpretability in Machine Learning – Principles and Practice' in Francesco Masulli, Gabriella Pasi and Ronald Yager (eds), *Fuzzy Logic and Applications. WILF 2013.* (Springer International Publishing 2013).
[689] 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 Duke Law and Technology Review. See also a related discussion in Section 5.4. of this thesis.
[690] Ibid.
[691] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 2.
[692] Dónal Doyle, Alexey Tsymbal, Pádraig Cunningham, 'A Review of Explanation and Explanation in CaseBased Reasoning' <https://scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-41.pdf> accessed 27 December 2018.
[693] Edwards and Veale (2017); Wachter, Mittelstadt and Floridi (2017).

The second subcategory, the *significance* of the decision, has two connotations: the objective and the subjective one. The *subjective* significance refers to an individual's own perception of the effect(s) of the automated decisions.[694] In the face of an increasingly automated and inhuman(e) data-driven world,[695] such subjective considerations should certainly be taken into account. For example, showing an appropriate ad that upsets someone could be subjectively significant. A drastic example comes from the US, where a woman was being shown advertisements for burial urns six months after her mother passed away.[696] The *objective* significance is established when a decision is regarded by a considerable number of other persons as significant.[697] For example, an automatic assessment of a financial situation by a bank may be viewed as banal by wealthy persons, but it may represent a significant decision for the people who financially depend on access to the bank loan.

Finally, *envisaged consequences* of automated decision-making relate to consequences that can be conceived as a possibility due to data processing.[698] In principle, these consequences refer to the opportunities and risks that individuals gain/take by sharing their data.[699] Risks are of particular relevance since in principle controllers tend to disregard them. Hildebrandt believes that the provision should be interpreted broadly.[700] In her view, the effects that are not intended but can be envisaged due to the generative nature of profiling must also be accessed and communicated.[701] Recently, social media networks have become a key source of information for recruiters. For two thirds of recruiters, LinkedIn is the most important social network for candidate sourcing.[702] Recruiters are able to employ LinkedIn's own search tools to select candidates to invite to a job interview. Putting this example into perspective, the social networks should provide users with information about the automated decision-making and about the risk of not being considered for a job. In this regard, Hildebrandt points out the important link between this requirement and the principle of purpose specification: *'the purpose specification principle is reinstated as an important legal rule, because envisaging effects requires ex ante specification of the targeted effects.'* [703]

Under Articles 13 and 14, the GDPR seems to guarantee an *ex ante* explanation but it does not include the explanation of a specific, individual decision that would be provided *ex post* data processing.[704] This drawback could be mitigated with some other provisions of the GDPR, for example the right to access

---

[694] Lee A Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Report 25.
[695] Inhumane here refers to both – consisting of artificial intelligence and lacking respect for human dignity.
[696] Rosiebita (@Rosiebita), 'Had the same situation with my mother's burial urn. For months after her death, I got messages from Amazon saying, "If you liked THAT urn, you might also like THIS one!"' (6 April 2018) <https://twitter.com/rosiebita/status/982293240261914625> accessed 16 June 2018.
[697] Bygrave (2001) 8. Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855> accessed 14 June 2018..
[698] 'envisage', Oxford Living Online Dictionary <https://en.oxforddictionaries.com/definition/envisage> accessed 14 June 2018.
[699] Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012) 51.
[700] Ibid.
[701] Ibid.
[702] Right management <http://www.kent.ac.uk/careers/jobs/social-networking.htm> accessed 5 June 2018.
[703] Hildebrandt (2012) 51.
[704] Wachter, Mittelstadt and Floridi (2017) point out the inappropriate use of the phrase – right to explanation. Namely, the right to have a decision explained is not provided anywhere in the binding GDPR text. There is a short reference in Recital 71, however this is not a binding text and the legislative history documents indicate that the legislator deliberately decided not to include it in the binding part.
[704] Wachter, Mittelstadt and Floridi (2017) 1.

in Article 15 and the right to contest the decision in Article 22.[705] Nevertheless, the new right to information on automated decision-making is a bright point in the GDPR. First of all, the provision has become a constituent part of the 'information catalogue', which increases the likelihood that data subjects will come across it. Second, if interpreted favourably, it could help establish a system of more accountable and transparent data processing by data controllers.

5.3.2. The quality of communication

Article 12 of the GDPR stipulates requirements in relation to transparency and modalities to facilitate individual rights. Paragraph 1 describes some distinct attributes of the communicated information by requiring that data controllers provide it '*in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'* In comparison to the DPD, this GDPR provision expressly requires data controllers to adopt a more transparent, user-friendly, and open approach.

Two sorts of requirements stem from the first paragraph of Article 12. The first relates to the quality of the form in which information is provided. This has to be concise, transparent, intelligible, and easily accessible. The second relates to the language, which has to be clear and plain.[706]

Concise means that information is given clearly and in a few words: brief but comprehensive.[707] Concise writing conveys the writer's points succinctly, without superfluous words, and with an appropriate level of detail.[708] The final result is that the text is clearer and more engaging for the reader.[709] For example, after being subject to a thorough review by the European data protection authorities, Google's privacy policy has been extended, however information is no longer provided in one single passage but structured in several paragraphs and bullet points to ease reading.[710] By using this layered format, it has become more concise.

A related requirement is intelligibility; *intelligible* stands for something that can be understood or comprehended. If 'concise' refers to the information itself, being intelligible necessarily involves a data subject. To be comprehended and understood, information has to be presented in a way that is suitable to the intellectual capabilities of a data subject. The bar should not be set high. In fact, it has been shown that the intelligibility for data subjects in the online environment has been highly limited.[711]

In principle, intelligibility has to be assessed according to the abilities of an ordinary person. However, fulfilling the right to (access to) *quality* information will sometimes require that we consider in what

---

[705] Edwards and Veale (2017) 35.

[706] In English, use of actives verbs, omission of legal jargon and sticking to the commonly used structure has been suggested as the optimal one. In other languages, a similar simplistic approach should be considered. Language properties also face challenges. One of them is use of English, which is a *lingua franca* of the Internet. Many data subjects are not native speakers of English, which means that they are more likely to run into some comprehension difficulties. Because of the internet jargon, language is a problem also for natives.

[707] 'concise' Merriam-Webster Online Dictionary <https://www.merriam-webster.com/dictionary/concise> accessed 4 June 2018.

[708] Mark Osbeck, 'What is "Good Legal Writing" and Why Does It Matter?' (2012) 4 Drexel Law Review 417, 438.

[709] Ibid.

[710] Lisa Mazzie Hatlen, 'Conciseness in Legal Writing' [2009] Wisconsin Lawyer, the official publication of the State Bar of Wisconsin. Also, conciseness is closely linked to the requirement to use clear and plain language.

[711] Among the reasons is technological complexity due to particular nature of data, information overload that complicates communication, and individuals' psychological limitations such as bounded rationality. See more in section 4.5.

format the information will be most comprehensible to one particular group of people. The following are two distinct situations in which the proper way of providing information plays a significant role:

a) where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom, and for what purpose personal data relating to him is being collected, such as in the case of online advertising;
b) where processing is addressed to a child (Recital 58).[712]

The complexity described under a) is an inherent part of the data-driven economy. For example, explaining algorithmic decision-making requires a different level of detail and simplification than providing contact information of a data protection officer.[713]

Easily accessible refers to the channels through which the information is retrieved. In the context of online privacy, it relates to the architecture of the website or electronic devices through which the information is provided. Article 12 stipulates that when appropriate, information should be provided in electronic form. One example of such a provision of information is through a website (Recital 58). Another option is access through a mobile app. Apps present a technology that can work to the advantage or disadvantage of a user who wants to be informed. On the one hand, app developers are often in the best position to provide notice and disclosure due to the proximity to the end-user.[714] On the other hand, lack of knowledge about privacy rules, limitations inherent in current mobile architecture, and dependence on third parties may undermine these good prospects.[715] The Article 29 Working Party has expressed fear that apps could disguise information important for a user: '[It] … *is unacceptable that the users be placed in a position where they would have to search the web for information on the app data processing policies instead of being informed directly by the app developer or other data controller*.'[716] For efficiency purposes, controllers should ensure that data subjects are aware of the decision-making system concerning them. This would not only benefit individuals but also public authorities, which could more easily assess the legality and ethics of an algorithm and the process through which a decision has been made. Indeed, a system that is not auditable is a system one should not use.[717] Hence, access to (understandable) information is as important as the information itself.[718]

---

[712] As regards b) the GDPR's Recital 58 makes a distinction between information that is provided to an adult and the information that is provided to a child. The latter should contain clear and plain language that the child can easily understand.
[713] Article 13(1)(b) of the GDPR.
[714] Future of Privacy Forum and The Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (2011) 1 <https://fpf.org/wp-content/uploads/Best-Practices-for-Mobile-App-Developers_Final.pdf> accessed 14 June 2018.
[715] Ibid.
[716] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' [2003] 23.
[717] See Mark Rotenberg's comment at the CPDP 2017 conference quoted by Hoepman, *supra* n 634.
[718] It should be borne in mind that data-driven algorithms can also be transparent and fair, even more than humans. Humans often make very biased decisions, are often not able to reliably 'explain' their decisions and are also hard to de-bias. See Gummadi's comment at the CPDP 2017 conference quoted by Hoepman, *supra* n 634. At the same time, the author also realises that there are many notions of fairness, and that a thorough mathematical formalisation of these notions showed that some notions of fairness are incompatible: they cannot be achieved both at once. A technological understanding of fairness can be different from a traditional legalistic understanding. For a technical understanding of fairness see for example Matt Kusner and others, 'Counterfactual Fairness', *1st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA* (2017).

The final requirement is *transparency*. In the ordinary sense, transparent means that there are no hidden agendas and that all information is available.[719] The dictionary definition in fact comes quite close to Recital 39, which describes transparency as an umbrella term for all other qualities of information listed above.[720]

In the data-driven economy, transparency is a challenging task. Three trends in particular are concerning. First, transparency can be threatened by the fact that data controllers are likely to conceal their methods, such as data mining and data sharing. Data mining details may be protected under intellectual property laws. The GDPR recognises the interest of companies in keeping the information about their internal decision-making processes confidential if disclosure would negatively affect their trade secrets, patents, or copyright-protected assets.[721] The reason for this provision is that forcing companies to reveal algorithms may clash with innovation objectives.[722] In addition, controllers are not explicit about those with whom they share information. In the aftermath of the Facebook and Cambridge Analytica scandal, it became obvious that Facebook users' data was shared with third-party apps on a daily basis – but only few users knew that their information was transferred all around the world.[723]

Second, transparency can be at risk because of the architecture of modern data processing systems, which sometimes do not allow for any meaningful explanation of their functionality. For instance, some types of AI analysis such as machine learning may yield unexpected, novel results that cannot be explained beforehand to data subjects because they develop gradually, learn from past decisions, and therefore become largely unpredictable.[724] For example, AlphaGo, Google's deep mind software, has been learning from its own experience, which makes it extremely difficult to understand its actions and to predict how the algorithm will behave in the future. During the latest battle between AlphaGo and a Chinese master, no one expected that the software could win. Only after AlphaGo's effortless performance did the developers realise how greatly its learning skills had improved and what sorts of decisions it had become capable of.[725]

Finally, transparency 'as a method to see, understand and govern complex systems' may sometimes be misleading or even actively unhelpful.[726] For instance, transparency of certain data mining processes may give an impression that they are sound, while the data that is being mined is in fact flawed and the outcomes unreliable. Because of this, it has been suggested that the focus of transparency in data-

---

[719] 'transparent' *Black's Law Dictionary* (1910).
[720] '*The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.'*
[721] Recital 63 of the GDPR. Here, the GDPR basically anticipates that non-disclosure would typically be required by IP laws anyway.
[722] Katja De Vries, Sari Depreeuw and Mireille Hildebrandt, 'D3.2 Profile Transparency, Trade Secrets and Intellectual Property Rights in OSNs – v1 (Deliverable for the USEMP Project)' (2015) 9.
[723] *Supra* n 628. During the hearing, the congressmen and the Facebook CEO discussed hidden facts related to Facebook's data sharing practice which, after they had become public, received strong disapproval.
[724] JA Kroll and others, 'Accountable Algorithms' [2016] U. Pa. L. Rev. 633, 638.
[725] Sam Byford, 'AlphaGo's battle with Lee Se-dol is something I'll never forget' *The Verge* (15 March 2016) <https://www.theverge.com/2016/3/15/11234816/alphago-vs-lee-sedol-go-game-recap> accessed 5 June 2018.
[726] Lilian Edwards and Michael Veale (2017) 34.

driven processes should not be on understanding the technical process, but on providing information that would enable data subjects to contest a decision[727] and to hold controllers accountable.[728]

While the GDPR's criteria on the quality of information surely suffer from multiple deficiencies, some positive steps forward have been made. In 2014, Custers, van der Hof, and Schermer examined privacy expectations of social media users and identified four criteria for decent privacy policies: 1) Is the information provided specific and sufficiently detailed? 2) Is the information provided understandable? 3) Is the information provided reliable and accurate? and 4) Is the information provided accessible? In the DPD, only criteria 1 and 3 were addressed to some degree. In the GDPR, all four criteria have been implemented.[729]

5.3.3. The form of communicating the information provisions

Regarding the form used to communicate the information to data subjects, the GDPR only provides some minimal hints. *Form* means the organisation, shape, and structure of something.[730] In terms of the shape, the GDPR mentions a few options: the information shall be provided in writing or by other means (e.g. icons, see section 5.3.3.1.1), and when appropriate by electronic means.[731] Given the increasing amount of data that is processed online, the electronic form should be prioritised. One example of the electronic form that the GDPR explicitly mentions is through a website (Recital 58). The alternative is providing information through a mobile app.[732]

With regard to the organisation, the information is typically communicated in one of the following two ways: as a privacy policy, or as part of general terms and conditions.[733] Below, these two means of organising the information function in the context of the data economy and their impact on individuals' control over personal data are assessed in more detail.

5.3.3.1. Privacy policies and/or notices

Privacy policies are internally focused tools that declare a company's policy regarding personal data use and how the company intends to achieve compliance with privacy principles.[734] Today, the majority

---

[727] Wachter, Mittelstadt and Russell (2018).

[728] boyd, danah, "Transparency != Accountability" (2016) EU Parliament Event 07/11 Algorithmic Accountability and Transparency <http://www.danah.org/papers/talks/2016/EUParliament.html> accessed 5 June 2018.

[729] van der Hof, Schermer and Custers (2014).

[730] It should be distinguished from methods. While the GDPR goes into detail of the quality of communication to data subjects (see section 5.3.2.), it does not elaborate on specific *methods* used to convey the required information. *Methods* stand for the procedure, technique, or way of doing something. The regulation maintains an open regime from the DPD, which left the implementation of the requirements up to data controllers. The directive made no distinction between actively communicating information about privacy practices and simply making it readily available to data subjects. Based on the unchanged wording and structure of the provision in the GDPR, this interpretation should uphold. Ustaran and International Association of Privacy Professionals (2012) 115.

[731] Article 12(1). When necessary, information may also be communicated orally, under the condition that the identity of a data subject is known.

[732] See also section 5.3.2. on 'quality of information'.

[733] Eleni Kosta, *Consent in European Data Protection Law* (Nijhoff 2013) 310.

[734] Contrary to privacy policies, privacy notices are externally oriented. If carefully designed, they should support objectives of transparency by alerting individuals as to what is being done with their personal data. Neil Robinson and others, 'Review of the European Data Protection Directive' (2009) <https://www.rand.org/pubs/technical_reports/TR710.html> accessed 6 June 2018. In comparison to privacy policies they are shorter and more concise. Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2012). In practice, the difference between notices and policies is often blurred and both words have been used to describe statements about a company's approach to protection of personal data.

of companies in Europe have a privacy policy.[735,736] While there is no explicit legal duty for a company's website to publish a policy, having one is usually the only practicable method of performing the company's informational duties towards users on the site.[737] This increased transparency was also mandated by industry self-regulation, as companies acknowledged stronger consumer demand for information.[738] Post-GDPR, many data-centered companies have made a noticeable move toward updating the language and format of their privacy policies.[739]

Policies are the main source of information for a data subject, in particular to help her decide whether to consent to data processing or not.[740] However, if consent is not used as a legal basis, this does not render privacy policies superfluous. They can be still important for those data subjects who would like to trigger their rights in relation to personal data, for instance the right of access or the right to object. Having meaningful information therefore plays a role that goes beyond consent.

Not only individuals but also other parties such as policy-makers, academics, researchers, investors, advocates, and journalists benefit from these disclosures.[741] Courts and DPAs tend to examine companies' online policies and/or statements especially closely in terms of whether they provide the necessary information and transparency.[742] European DPAs have demanded changes to Facebook', Tinder's, Google's, and Microsoft's policies.[743] It is important to note that investigation of privacy policies often requires a joint effort by several authorities.[744]

As mentioned, providing information and obtaining consent typically form an indivisible whole. Consent is a highly problematic concept, and this also has consequences for the provision of information. The idea of consent was introduced in data protection law to facilitate data subjects' active choice and control, but it somehow missed that goal. Due to the increasing number of consent requests in today's world, users often do not really consider the questions asked, do not read the information provided, and do not seem to think through the consequences of providing (or refusing)

---

[735] Mark Gazaleh, 'Online trust and perceived utility for consumers of web privacy statements' *(wbsarchive.files.wordpress.com,* August 2008). See also ARA Bouguettaya and MY Eltoweissy, 'Privacy on the Web: Facts, Challenges, and Solutions' (2003) 1 IEEE Security & Privacy 40.

[736] In some exceptional cases the information duty can be fulfilled in some other ways, meaning, neither in writing nor electronically. An example is when information is provided through a provision in a law. This exception is expressly provided in articles 12 and 13 of the GDPR.

[737] Kuner (2012) 283.

[738] Ibid.

[739] However, multiple updates preceding 25 May 2018, pointing at new privacy-protecting measures, proved counter-productive. The result was an information overload contributing to confusion of data subjects rather than increased transparency. For a critical view see Esther Keymolen, 'Jouw privacy is belangrijk voor ons', *(Bij Nader Inzien,* 23 May 2008) <https://bijnaderinzien.org/2018/05/25/jouw-privacy-is-belangrijk-voor-ons/> accessed 30 May 2018.

[740] Kosta (2013) 215.

[741] See more in: Mike Hintze, 'In Defense of the Long Privacy Statement' (2015) 76 Maryland Law Review 1044.

[742] Kuner (2012) 282.

[743] See for instance the report by Alsenoy and others (2015) that was used as a basis for the investigation in Belgium. Samuel Gibbs, 'Facebook disputes Belgian tracking order over use of English in court ruling' *The Guardian* (29 January 2016) <https://www.theguardian.com/technology/2016/jan/29/facebook-belgian-tracking-english-court-ruling-cookie-browser> accessed 6 June 2018. In relation to Tinder see n 232. In relation to Google see the letter from the Article 29 Working Party from 23 September 2014 <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf> accessed 6 June 2018. The Article 29 Working Party also sent a letter to Microsoft regarding some privacy issues in their service agreement.

[744] See for example the Article 29 Working Party's letter to Google regarding their Google glass technology signed by several data protection authorities worldwide <https://www.cnil.fr/sites/default/files/typo/document/Letter-to-Google-regarding-Glass.pdf> accessed 5 June 2018.

consent; rather, they simply consent whenever confronted with a consent request.[745] If, for this reason, consent has no more meaning for data subjects' control, the same goes for the right to information that is attached to consent. Thus, it is not surprising that privacy policies as a form of communicating information have received much criticism.[746]

A few solutions have been considered to address these drawbacks and some of them have been implemented in the GDPR. These solutions do not set a new paradigm, but instead represent a sort of replacement for traditional privacy policies. The first one is the use of icons and labelling as a means to more effectively communicate privacy policies. In Article 12 of the GDPR, controllers are explicitly allowed and given an option to use icons as a replacement for written policies. The second solution is the use of standardised contract terms or templates in business-to-consumer (B2C) relationships. Standardised policies were part of some previous versions of the GDPR but do not appear in its final text. Each of the two alternatives is briefly considered below.

5.3.3.1.1. Icons and other visualisations

Icons are symbolic or graphic representations of (parts of) privacy policies that convey information at a glance. As such, they could be one possible response to the failure of privacy policies in the data economy, which are typically too long and too complex to provide meaningful information. Icons could be beneficial for two reasons in particular: first, they simplify understanding of the information, and second, they save readers time. The idea is explicated in Article 12(7) of the GDPR, which contains the option to use standardised icons. Recital 58 adds that visualisation should be used *'where appropriate'.* Icons offer an alternative approach that intends to make privacy policies more accessible to a layperson.

The GDPR does not offer much guidance concerning the icons. Article 12(7) states that the information from Articles 13 and 14 may be provided in combination with standardised icons to provide a meaningful overview of the intended processing in an easily visible, intelligible, and clearly legible manner. The article further stipulates that where the icons are presented electronically, they shall be machine-readable.

The European Commission has been entrusted with drafting the detailed guidelines on icons.[747] It is plausible that its draft will rely on the foundation set by the LIBE version of the GDPR, which introduced, in Annex 1, a first sketch of privacy icons.[748] However, it remains to be seen what approach the EC will take in the future.

---

[745] Schermer, Custers and van der Hof (2013) 1.

[746] The problem is exacerbated on mobile sites where reading long policies is impractical. Lilian Edwards and Wiebke Abel, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors' (2014) 6 <https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf> accessed 6 June 2018.

[747] In the original version of the proposal the Commission's role to adopt delegated acts was considerably broad (*supra* n 30, see for instance articles 14(7), 15(3), 17(9) and 20(5) of the proposal). Not only was the Commission authorized to specify the use of icons, it was also assigned some other standardisation tasks. In the LIBE (Parliamentary) version, the Commission maintained those powers, but was more dependent on the European data protection board composed of national DPAs. Namely, the Parliament believed that DPAs have more specific practical knowledge and are therefore more capable of setting appropriate criteria. *Supra* n 662. In the final, adopted version, the EC's influence shrank again as the version additionally limited the number of delegated acts.

[748] *Supra* n 662.

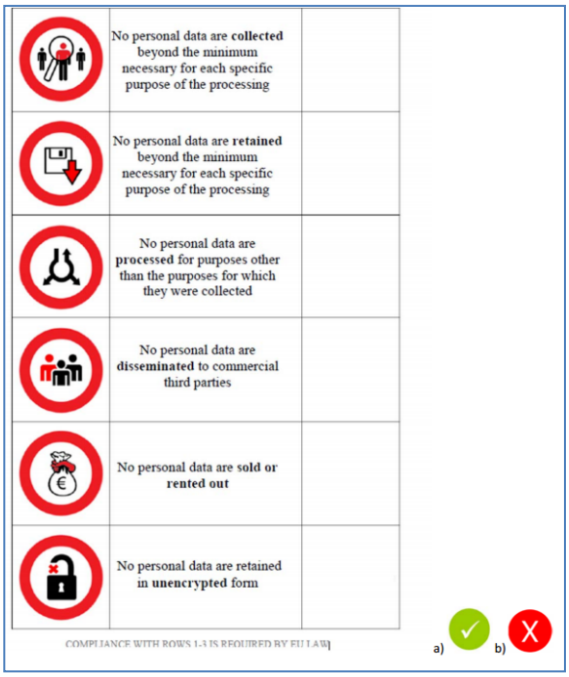

Figure 2: Privacy icons

The EC delegated acts are not the only source that companies can use to ensure that their policies are more user-friendly. Some alternative tools are also available, such as 'visuele voorwaarden' (visualised terms and conditions): a visualisation strategy created as part of a research project funded by the city of The Hague.[749] Visualisation has also been suggested as a possible way to include information on automated decision-making in a privacy policy.[750] A similar approach is to embed a privacy policy in a video.[751] Finally, information on data protection can also be provided in a more innovative manner. One example is to present a policy as a sort of nutrition label in a standardised tabular format to allow users to learn where to look to find information in a consistent location, and to facilitate comparison between policies.[752] The second example is policy compressed into a graphical representation of data flows built on AI textual analysis.[753]

Research indicates that visualisation can help some consumers better understand complicated data flows. Cranor's study found that in the condition without privacy icons, most participants made their purchases from the least expensive websites. However, in the conditions where privacy indicators were present, a significant number of participants paid extra to buy the items from the more privacy-protective web sites.[754]

---

[749] Janneke Boerman, 'Visual legal privacy statements' Presentation at the Open Minded (Leiden, Centre for Law and Digital Technologies (eLaw), 26 May 2016). For the visualization see <https://share.proto.io/FBR87S/> accessed 6 June 2018.
[750] Edwards and Veale (2017).
[751] The Guardian Privacy Policy <https://www.theguardian.com/info/video/2014/sep/08/guardian-privacy-policy> accessed on 6 June 2018.
[752] Lorrie Faith Cranor, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2011) 10 Journal on Telecommunication & High Technology Law 273, 288.
[753] <https://pribot.org/polisis/> accessed on 6 June 2018.
[754] Lorrie Faith Cranor (2011) 292.

In solving the problems of information overload, lack of sufficient time and attention devoted to privacy-related information, and lack of digital literacy, icons and similar simplification methods could play a key role. As stated above, icons are beneficial for two reasons. First, they dramatically reduce the information overload that consumers face in the contemporary online environment. Closely related to this, they decrease information complexity. As a result, less time and attention are necessary for consumers to grasp the implications of the disclosure of their personal data.

The drawback is that icons do not provide comprehensive knowledge about data collection practices: they only provide information in a manner that is highly generalised and simplistic. By using a standardised language that signals trust, consumers may be less susceptible to the fact that they only receive partial information. However, in the data economy, it is the hidden and intangible details that carry significance rather than some general information.[755] By focusing too much on providing easy-to-understand information, individuals might be tempted to take suboptimal decisions.[756]

5.3.3.1.2. Standardised privacy policies

A regulated privacy policy in a standard form has been recommended as an effective means to ensure that consumers are sufficiently protected against industry terms that are unfair and/or significantly weighted in favour of the provider.[757] Regulating the shape of a contract is an approach that has similar consequences as icons: decreasing complexity of policies, cutting down the time needed to review the terms, and generating control for consumers (including related aims such as trust and confidence). The GDPR icons mentioned in the previous section are an example of visualised standards. Likewise, standardisation is possible for textual policies. For example, the US Glemm-Lech bill's annex provides a privacy policy template for financial institutions.[758] The LIBE version of the GDPR suggested a similar approach for privacy policies.[759] However, this provision was removed from the adopted version of the GDPR.[760]

Building on the American experience, Cranor speaks strongly in favour of standardisation.[761] She believes that the digital online environment can be a good facilitator of standardisations since

---

[755] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140 Dædalus, the Journal ofthe American Academy of Arts & Sciences 32, 36.

[756] For example, an icon may state that no personal data is sold to third parties. However, aggregated data might still be sold and may have adverse privacy or other implications.

[757] Edwards and Abel (2014) 31.

[758] <https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf> accessed 6 June 2018.

[759] *Supra* n 662, Amendment 109. Such standardized policies/notices would include the information on whether:

- personal data are collected beyond the minimum necessary for each specific purpose of the processing;
- personal data are retained beyond the minimum necessary for each specific purpose of the processing;
- personal data are processed for purposes other than the purposes for which they were collected;
- personal data are disseminated to commercial third parties;
- personal data are sold or rented out;
- personal data are retained in encrypted form.

[760] An important addition in the LIBE version was that privacy policies should be provided in a layered form. In a layered privacy notice, basic information is provided in a short initial notice and further, more detailed information is available should an individual want it. Layered privacy notices provide an ideal way, particularly in an online context where, click through links can be adopted by providing a simple way for the data subject to access more detailed information. Supra n 662, Amendment 109, Article 13(a)(2). Also see Ustaran and International Association of Privacy Professionals (2012) 120-121.

[761] Which would, similarly as food labels, educate consumers about possible risks.

machine-readable policies allow for more standardisation and better comparison. In fact, open software already exists that supports comparisons and assessments of privacy policies.[762]

However, it cannot be excluded that visualised or standardised privacy policies could suffer from similar drawbacks as the non-standardised: either they could become too generalised and therefore miss some important details,[763] or they could become too detailed and impossible to follow.[764] More importantly, to be effective, standardised notices need to have fairly rigid requirements so that their elements are directly comparable.[765] To achieve this, a considerable amount of regulatory effort is indispensable. Ideally, standardisation is triggered by law (international treaty), by industry groups, or by standard setting bodies such as the ISO.[766] All these strategies require a lengthy negotiation process with many compromises and, as seen in the GDPR example, no guarantees of actual positive outcomes.

5.3.3.1.3. Information incorporated in standard terms and conditions

Privacy policies are by far the most common approach to inform data subjects online. However, this is not required under the GDPR. Instead of using privacy policies, some companies may choose to provide the information on personal data processing in their standardised terms and conditions (STC). The STC stand for a contract between two parties, where the terms and conditions of that contract are set by one of the parties and the other party has little or no ability to negotiate more favourable terms and is thus placed in a 'take-it-or-leave-it' position.

In principle, a privacy policy provided as part of a contract should not be considered unusual. When consent is the ground for fair and lawful processing, it is actually easy to put any data protection practice into a contract and legitimise it through acceptance of the contract.[767] However, the Article 29 Working Party advises against inserting the information in the general conditions of the contract,[768] as in digital services consent is often routinised and automatic.[769]

However, even if there is a privacy policy in place, terms and conditions might still be a source of information important to a data subject, as they might indirectly relate to the subject's privacy. For example, Twitter's APIs[770] allow developers to use Twitter's data streams.[771] A data subject can only fully understand all the risks of personal data processing by receiving the information about developers' possibilities to reuse data. In certain cases, for instance, deletion of tweets that include personal data is not absolute, as the data has already been shared with developers.[772] By combining the privacy policy and the terms, a data subject can see a more holistic picture.

---

[762] See for instance <https://tosdr.org>.
[763] Hintze (2015) 16.
[764] Omri Ben-Shahar and Carl Schneider, *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014).
[765] Cranor (2011) 305.
[766] Edwards and Abel (2014) 4.
[767] Ibid., 6.
[768] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) 14.
[769] Edwards and Abel (2014) 6.
[770] API stands for application program interfaces.
[771] Twitter's Developer Agreement <https://developer.twitter.com/en/developer-terms/agreement> accessed 6 June 2018.
[772] Helena Ursic, 'The Right to Be Forgotten or the Duty to Be Remembered? Twitter Data Reuse and Implications for User Privacy' (2016) <https://bdes.datasociety.net/wp-content/uploads/2016/10/Ursic-politiwoops.pdf> accessed 6 June 2018.

5.3.4. Timing

5.3.4.1. When in time?

If personal data is not obtained from a data subject but from a third party, the controller has to ensure that information is received before that data is disclosed to a recipient (Article 14(3)) or at the time of first communication with the data subject if communicating is the primary reason for data processing (Article 14(2)). In other situations, the data subject has to be informed within a reasonable period, at most one month (Article 14(1)).[773]

The differences between the situations could create an interesting discrepancy. If a data controller does not intend to disclose the data (i.e., share the data with a third party), data subjects must be informed within a reasonable period, at least within one month. If the controller records the data with the intention of disclosing (sharing) it at some point, a situation which is more likely to have a significant impact on the data subject, providing the information may be delayed until the time of disclosure, however distant this might be.[774] In today's data-driven economy, where privacy risks occur mostly when data is shared and disclosed, distinguishing the situations in this manner could raise concerns.[775] To protect data subjects, the provisions should be read cumulatively.

5.3.4.2. How often in time?

In cases when data is collected directly from a data subject, the information needs to be provided at the moment of data collection (Article 13(1) of the GDPR). This information must be updated if the purpose of the data processing changes (Article 13(3)). For example, if a communication service provider starts using individuals' location data to make predictions about their shopping habits to place ads instead of using it for billing purposes only, data subjects should receive an update about that new purpose.

A distinct question is what happens if not the purpose but some other aspect of data processing changes**.** The Norwegian Consumer Council's (NCC) report supports a broader interpretation, under which all updates should be communicated*: 'Especially in the case of material changes, including functionality and user rights, the services should provide advance notice, so that anyone who does not agree to the new terms has an opportunity to export their data, leave the service, and potentially find*

---

[773] *'It must, however, be observed that that provision, which concerns data which have not been obtained from the data subject, provides for information to be provided to the data subject not at the time when the data are obtained but at a later stage. By contrast, Article 10 of Directive 95/46, which refers to the collection of data from the data subject, provides for the data subject to be informed at the time the data are collected […]. The immediate nature of the provision of information to the data subject thus comes not from Article 11 of Directive 95/46, mentioned by the referring court, but from Article 10.'* Case C-473/12, *IPI v. Geofrey Engelbert* ECLI:EU:C:2013:715 (7 November 2013), para. 23.

[774] Douwe Korff, 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws' (2002) <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> accessed 6 June 2018.

[775] On a similar note, one could raise doubts in the system in which the timing of the communication with a data subject is based merely on the fact whether data is obtained from a data subject or not. Apart from some practical difficulties that controllers could face, there is no reason to demand that in one case information is provided right away while in the other (and potentially more invading) situation, the provision of information can be delayed for a few weeks. For example, communicating information about future recipients of data is necessary before data is obtained from a data subject. In cases when data is received from a third source, however, article 14(3)(c) suggests that this can be done up to the moment when data is disclosed to a new recipient.

another provider before the new terms are put into effect.'[776] To summarise, in the NCC's view material changes should always be communicated, but a note to consumers should not be ruled out in the case of minor changes.

The Article 29 Working Party believes that it is a precondition for the exercise of data subject rights that individuals be continuously kept informed, not only when they subscribe to a service but also when they use it. For example, if a service requires ongoing processing of location data, the Working Party takes the view that the service provider should regularly remind the individual concerned that her terminal equipment has been, will be, or can be located. This allows that person to exercise the right to withdraw, should she wish to do so.[777] In line with the Working Party's view, any other relevant change that might urge data subjects to withdraw or block certain processing of personal data should also be regularly provided as an information update.[778]

5.3.5. Restrictions

Because the right to information is a manifestation of the fundamental right to data protection and some other fundamental principles,[779] every exception has to be used with the utmost prudence and care. According to the settled case law, *'the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.'*[780]

The GDPR's provisions on exceptions try to establish the right balance between legitimate interests of data controllers and protection of data subjects. The most obvious exception to information duty applies when a data subject already has all the information to which he is entitled (Article 13(4)). In such cases, providing the information for the second time is neither necessary nor economical.

In cases when data is *not* obtained directly from a data subject, the GDPR offers some further exceptions in addition to the one explained in the paragraph above. For example, the information duty is limited if it would require disproportionate effort, especially when data is used for archiving in the public interest, for scientific or historical research purposes, or for statistical reasons.[781] Consider researchers employing a medical data set for new scientific research unrelated to the data's original use. Given the size of the database and, more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually to provide them with the information on the new purpose of use of the database.[782] Thus, an exception should apply.

---

[776] Forbrukerradet, 'Consumer Protection in Fitness Wearables' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf> accessed 5 June 2018.
[777] Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' 33.
[778] Ibid.
[779] Such as transparency and fairness. See section 5.2. of this chapter for more detail.
[780] See for example Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, paragraph 56, and Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paragraphs 77 and 86.
[781] Article 14(5)(b) and (c). The scope of 'scientific research' is not clear. Whether pharmaceutical research also falls under this exception is open to discussion. According to the interview with a pharmaceutical company representative, if the RWE initiative is not scientific research *per se*, it could be at least something *that adds to scientific research*. In this way, also pharmaceutical research could fall under the umbrella of Article 14. Liliya Pullmann and others (2017) 32-33.
[782] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) 31.

Interpreting open terms such us 'disproportionate' can be challenging in certain cases. Should disproportionate be understood objectively or subjectively? Disproportionate effort has a different connotation for a large commercial company that plans to utilise personal data to increase sales than for an understaffed academic centre. Through the eyes of the Google Spain court, balancing fundamental rights should disregard economic difficulties of a data controller.[783] It is likely that the bar to avoid information duties should be set higher for commercial companies.

The exceptions listed above are specific to the right to information. Article 23 of the GDPR contains an additional set of exceptions such as national security and public interest that are applicable to all data subject rights.[784] Therefore, they should also be read jointly with Articles 13 and 14.

5.4. The right to information in the electronic communication sector

5.4.1. Privacy of electronic communication

Therefore, the information duty from the GDPR applies equally to all controllers of personal data regardless of sector. However, protection of personal data in the electronic communication sector is additionaly safeguarded by ePrivacy rules. Inasmuch as the ePrivacy rules provide specific rules in relation to electronic communications, this additional or special provision should also be taken into account on top of the GDPR rules. This situation is a specific application of the doctrine stating that a 'law governing a specific subject matter (*lex specialis*) overrides a law which only governs a general matter (*lex generalis*).'[785]

The current 2002 ePrivacy directive will soon be replaced by a new regulation intended to bring (sometimes clashing) national legislations closer to each other.[786] At the time of writing, the text of the regulation was still in the legislative procedure, but based on the EC proposal some of the positive and the negative points could already be assessed.[787] The text below provides an overview of the ePrivacy

---

[783] '*In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing*.' C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

[784] Under Article 23 of the GDPR restricting data subject rights may be allowed under the principle of proportionality. In other words, the restricting measure has to be laid down by law, respect the essence of the fundamental rights and freedoms, and fall under the limits of proportionality test, i.e. be necessary and proportionate in a democratic society to safeguard the following objectives:

- national security;
- defence;
- public security;
- criminal prevention and enforcement
- other important objectives of general public interest of the Union or of a Member State e.g. financial or economic interests
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

[785] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' 10.

[786] In the system of EU law, regulation is a type of law that intends to unify rather than harmonize national legislations. In other words, when a regulation is adopted its text is in principle directly implemented in member states. Directives, on the other hand, are only binding as far as their goals are concerns, but still allow for divergences.

[787] *Supra* n 468.

law in relation to information rights, drawing mainly on the ePrivacy directive. When specific provisions are discussed, it is indicated whether the directive or the regulation is referred to.

The ePrivacy rules concern four types of data processing: (1) processing of traffic data, (2) processing of location data, (3) using electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user, and (4) other uses, such as unsolicited messaging and telephone calls as part of direct marketing, and inclusion in public directories.

In the context of the data-driven economy, the last type (4) is less relevant. The other three, however, represent an integral part of modern personal data processing, especially in the online environment. To illustrate the application of the right to information in the electronic communication sector, the following sections briefly introduce the information duty in relation to the third type (3) of e-communication data processing. Within this group, it is possible to distinguish two types of processing: (a) storing information in the terminal equipment of a subscriber, and (b) gaining access to the information stored therein.[788]

5.4.2. Informing about placing the cookies and location tracking

Within the scope of (3) above (storing information in the terminal equipment of a subscriber), ePrivacy provisions restrict the use of cookies and/or similar technologies (e.g. web beacons, Flash cookies, etc.)[789] stored on users' computers to track their online behaviour.[790] This type of personal data processing is a building block of the e-commerce online advertising business. By storing a cookie on a user's computer, advertisers obtain a precise understanding of this person's actions on the Internet. As a consequence, they are able to direct their ads to the most interested (or most vulnerable) consumers and therefore increase their sales. Considering the exponential growth of the e-commerce sector, it is likely that online behavioural advertising and the use of cookies and similar technologies will expand in the future.[791,792]

Under current (and upcoming) ePrivacy rules, deploying cookies is only allowed if data subjects have consented to it and if they have *'been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing'*[793] Thus, providing information and obtaining consent form an indivisible whole. Informing the data subject should take

---

[788] See Article 5(3) of ePrivacy directive.

[789] A web beacon is a small, invisible object such as a tiny clear image that is the size of a pixel embedded into a web page. When a web page with this image loads, it will make a call to a server for the image. This is very useful to companies that want to learn if readers are opening the emails they send. A flash cookie is a piece of information that Adobe Flash might store on your computer to save data such as video volume preferences or, perhaps, your scores in an online game. Flash cookies are more persistent and cannot be deleted in the same way as other cookies. Joanna Geary, 'Tracking the trackers: What are cookies? An introduction to web tracking' *The Guardian* (23 August 2012) <https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro> accessed 23 September 2018.

[790] See Article 5(3) of ePrivacy directive and Article 8 (1) of the proposal for the ePrivacy regulation.

[791] Robert Gebeloff and Karl Russell, 'How the Growth of E-Commerce Is Shifting Retail Jobs' *The New York Times* (6 July 2017) <https://www.nytimes.com/interactive/2017/07/06/business/ecommerce-retail-jobs.html> accessed 6 June 2018.

[792] Recently, researchers have found that 100 most popular sites collect more than 6,000 cookies, of which 83% are third-party cookies, with some individual websites collecting more than 350 cookies. Ibrahim Altaweel, Nathaniel Good and Chris Jay Hoofnagle, 'Web Privacy Census' [2015] Technology Science.

[793] Article 5(3) of the e-Privacy directive. The proposal for the ePrivacy regulation refers to the GDPR's provision on the right to information (Article 8(1)(b) of the proposal).

place before the server of a controller sends the cookie to the Internet user's hard disk.[794] In practice, this is normally done by using a cookie banner. Cookie header banners are displayed on websites using cookies and require consent if a user wants to proceed to the website. Such cookie banners easily turn into a 'take-it-or-leave-it' option. As a result, the majority of users consent whenever they are confronted with a cookie wall.[795] Due to lack of *informed* consent, it has been suggested that tracking walls should be banned, at least in certain circumstances.[796] Instead, browser and comparable software settings could play a role in addressing this problem. For instance, it has been argued that browsers could be set to privacy-friendly settings that limit online tracking.[797]

Besides the medium used to convey the information, the content of the message is equally important. In relation to automated online data collection (e.g. cookies), the Article 29 Working Party suggested that data subjects should be provided not only with the standard set of information listed in Article 13 of the GDPR, but also with some extra items.[798] In a document from 2013, the Working Party stated that the necessary information regarding cookies includes the purpose(s) of the cookies and, if relevant, an indication of possible cookies from third parties or third-party access to data collected by the cookies on the website.[799] For example, if a cookie is used to remember in what language version an Internet user wants to access a website, then the information should explain that and notify the user that the next time he visits he will not have to repeat his choice, since it will be remembered by the cookie.[800] In addition, if the information is gathered or processed by third parties, then this fact should be pointed out specifically to Internet users.[801] Marketers should also convey additional information (or link to it) regarding who that third party is and how it may use the information.[802] Information such as retention period (i.e. the cookie expiry date), details of third-party cookies, and other technical information should also be included to fully inform users.[803] Finally, in the Working Party's view, users must be informed about how they can signify their wishes regarding cookies, i.e., how they can accept all, some, or no cookies, and how they can change this preference in the future.[804]

Tailoring the information to the nature of a specific technology is a good strategy that should be adopted for other technologies as well (e.g., Wi-Fi tracking, face and voice recognition by IoT devices). However, informing users about cookies leads to exactly the same problems as any other type of

---

[794] Article 29 Data Protection Working Party, 'Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data on-Line in the European Union' 6.

[795] Frederik Johannes Zuiderveen Borgesius and others, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (2017) 87 <https://www.ivir.nl/publicaties/download/IPOL_STU2017583152_EN.pdf> accessed 17 November 2017.

[796] Ibid., 89. Negotiations on whether cookie walls should be prohibited or not are still ongoing.

[797] Ibid., 8.

[798] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' 3.

[799] UK Information Commissioner Office, 'Guidance on the Rules on Use of Cookies and Similar Technologies' 21 <https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf> accessed 17 November 2017.

[800] Ibid.

[801] Ibid., 22-23.

[802] Ibid.

[803] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' 3.

[804] Ibid. See also International Chamber of Commerce UK, 'ICC UK Cookie Guide' <https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf> accessed 7 June 2018; Informacijski pooblaščenec Republike Slovenije, 'Kdaj Lahko Uporabimo Piškotke? Smernice Informacijskega Pooblaščenca' <https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf> accessed 7 June 2018.

communication to data subjects. When the information is short and summarised, some important details may be missed, while when it is long and detailed, it is perceived as a burden and often disregarded. Although there is no simple solution to data subjects' disinterest, providing a complete set of facts is not useless. The information may be useful to regulators, journalists, and the general public, and thus work as an important indicator of a controller's accountability.

5.4.3. Informing users about Wi-Fi tracking

Within the scope of (3)(b) above (gaining access to the information stored in a subscriber's terminal equipment) ePrivacy law regulates location tracking on the basis of Wi-Fi or Bluetooth signals emitted by people's smart phones. Under the ePrivacy directive, this is only allowed if data subjects have consented to it and have been provided with clear and comprehensive information. Under the proposed ePrivacy regulation,[805] such tracking is allowed under somewhat relaxed conditions (Article 8(2)). Article 8(2) states that in order to inform those who are being tracked, it is sufficient to display a clear and prominent notice, e.g. hang a poster with information about the tracking. This means that collection of valuable data is in principle possible without the hassle of obtaining individuals' consent. Some retail stores have already successfully embraced this as the new technique to monitor shoppers.[806] For this reason, Article 8(2) has been fiercely criticised for not sufficiently allowing data subjects' control and intervening with some broader privacy objectives. Clearly, providing a poster with some general information does not resolve privacy risks in relation to tracking. *'Under that proposed rule, people might never feel free from surveillance when they walk or drive around. People would always have to look around whether they see a sign or poster that informs them of location tracking*.'[807] The Article 29 Working Party assessed the proposal and issued a negative opinion, urging the legislator to only allow Wi-Fi tracking on the basis of informed consent.

5.4.4. Information on cybersecurity

The draft ePrivacy regulation introduces a new obligation for electronic communications service providers to provide information about the security of their technology, e.g. about using encryption. Article 17 stipulates: '*In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken*

---

[805] *Supra* n 468.

[806] *'Everything from where they go, what they look at, how long they engage with a product and whether all this ultimately results in a sale, can all be anonymously monitored and used to make each experience more personal.'* Sarah Knapton, 'High street shops secretly track customers using smartphones' *The Guardian* (27 December 2016) <http://www.telegraph.co.uk/science/2016/12/27/high-street-shops-secretly-track-customers-using-smartphones/> accessed 7 June 2018.

[807] Zuiderveen Borgesius and others (2017) 8. Another degradation of data protection related to the information duty can be spotted in Article 10 of the proposed ePrivacy regulation from December 2016. The draft proposal that was leaked in December required that any setting of terminal equipment (e.g. personal computer, mobile phone) must be configured in a way that prevents third parties from storing information in this equipment, or to use information that has been stored there. In essence, the requirement demanded that third party cookies, which are the backbone of the targeted advertising industry, should be blocked by default. The later proposal abolished this requirement. Rather than requiring that the software is set to "do not track", privacy-friendly mode, the official proposal only requires that it *offers an option* to do so and provides information about this option. Again, the provision was criticized as it is obvious that merely informing someone offers far less privacy protection than creating privacy-enabling software architecture. Helena Ursic, '"The bad" and "the good" of ePrivacy proposal' (*Leiden Law Blog,* 19 January 2017) <http://leidenlawblog.nl/articles/the-bad-and-the-good-of-the-eprivacy-regulation-proposal> accessed 3 June 2018.

by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.' According to Recital 37, this information should be provided free of charge.

Given the rising number of cyber risks, stronger reference to security can have positive consequences for data subjects' awareness and control. However, it has been argued that ePrivacy regulation is not the best setting to regulate cyber risk.[808] Notably, cyber security is already addressed in some other legal acts, including the GDPR.[809] Lack of reference to these acts in the ePrivacy regulation might be puzzling. In addition, security of devices is a technical and complicated topic that cannot be thoroughly dealt with in the ePrivacy regulation.[810]

5.5. The right to information as a control affording entitlement

This section summarizes some key barriers and enablers to providing meaningful information that have to some extent already been crystallised in the previous sections. The aim is to assess the degree to which the right succeeds or fails at helping data subjects exercise control over their personal information.

5.5.1. Limits to data subjects' control

In section 4.5, it was suggested that three groups of factors – psychological, technological and economic – seem to undermine the effectiveness of data subject rights and escalate data subjects' inability to control information flows. As shown in section 5.1.-5.4., these same factors also have implications for the right to information. The barriers to providing effective information stem from individual psychological patterns, the specifics of data-driven technologies, and the modern economic environment.

Psychological factors. The ubiquity of personal data processing in combination with the information duty has resulted in the phenomenon of informational overload. Today, the majority of modern devices, media, and services use personal data. Since almost every use of personal data triggers the right to information, consumers are confronted with major amounts of information about their personal data processing daily. The continuous (though partial) attention to an increasing amount of information decreases data subjects' ability and motivation to scrutinise the key details that are necessary to make informed privacy decisions. Paradoxically, the more information they receive, the less information they are able to filter, process, and weigh to make decisions that are in line with their preferences.[811] Further, limitations in general cognitive abilities and low 'literacy' prevent data subjects from understanding the complex policies' language.[812] The phenomenon of 'bounded rationality' also adds to the problem: this concept confirms that judgements and decisions are often not reached on the basis of a rational *optimisation process*, but are instead the result of heuristic and biased

[808] Zuiderveen Borgesius and others (2017) 106.
[809] Notably the NIS directive, *supra* n 475.
[810] Ibid.
[811] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016.
[812] Eszter Hargittai, 'Whose Space? Differences Among Users and Non-Users of Social Network Sites' (2008) 13 Journal of Computer-Mediated Communication Whose 276.

information processing.[813] For example, the mere existence of a privacy policy signals trustworthiness, which in turn decreases privacy concerns and increases disclosure behaviour.[814]

Technological fators. The intangible and invisible nature of personal data opens up possibilities to duplicate and share in an opaque and less controlled way than physical goods. This specific technical nature of data challenges the simple disclosure mechanisms suggested in the GDPR. It is the hidden and oftentimes highly technical details that carry significance.[815] The Article 29 Working Party describes this problem in a mobile app environment. While apps can have extremely broad access to sensors and many other data structures on a device, in many cases this access is not intuitively obvious.[816] Moreover, after data is collected, it can easily flow to third-party data controllers or processors, where it is combined and/or reused.[817] The route that personal data takes is difficult to follow. Often, even the data collector itself is ignorant of the parties that eventually receive it.[818] This of course challenges transparency of data processing. Simplifying privacy policies by using plain and concise language as suggested in the GDPR will probably make them easier and quicker to read, thus mitigating the psychological problem of information overload and bounded rationality, as described in the previous section.[819] However, when it comes to the complexity of data flows, simplification is not of much help. Control will almost never stem from the information provision, but will only come from external overseeing of data processing practice such as academic research and enforcement checks.

Economic factors. Finally, the right to information is challenged by the diffusion of responsibility. In the modern data economy, the tendency to reuse data creates a network of multiple actors involved in the processing of the same data. This technical diffusion of responsibility is also economically incentivised by the underlying business models such as behavioural advertising.[820] Consequently, the duty to inform becomes dispersed. For example, data can be purchased from a third party, such as a data broker, and can then be curated, repackaged, and sold to another party. In such cases, a data subject often has no interaction with the actual controller.[821] Although individuals maintain the right to information, the timing and the scope of the received information is influenced by the fact that data flows through a network of (joint) controllers and processors. When information is received from a third party, the set of information is to some extent limited and is not presented directly to a data subject.[822] Clearly, such

---

[813] Gigerenzer and Selten (2002).

[814] A study by Hoofnagle and Urban found that 62% of respondents to a survey believed that merely the existence of a privacy policy on a website implied that this website was not allowed to share their personal information without permission. Chris Jay Hoofnagle and Jennifer M Urban, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest L. Rev. 261.

[815] Nissenbaum (2011) 36.

[816] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' 22. Also see Section 5.4.3. of this chapter.

[817] Ellen Nakashima, 'Prescription Data Used to Assess Consumers' *The Washington Post* (4 August 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080302077.html> accessed 5 June 2018.

[818] Ursic (2016). Also see hearing of Mark Zuckerberg in the US Congress on April 10, 2018 (n 642) for the report on apologies made by Facebook CEO Zuckerberg for not discovering inappropriate data flows triggered by Cambridge Analytica's app.

[819] The problem of bounded rationality will be difficult to solve with the measures that supposedly increase the scope or quality of communication. Rather, a modification of the software architecture should be deployed as the solution – for instance, a default option that is privacy friendly and an opt in requirement. However, under the pressure of the industry lobby, regulators are typically hesitant in adopting such radical measures.

[820] Section 2.3.3.

[821] See section 2.3.1. in relation to the data brokers' business model.

[822] See section 5.3.1.1.

conduct decreases control over data processing. Furthermore, exceptions to the right enable controllers to escape the information duty when it would involve disproportionate efforts.[823] As it appears, the disproportionality is most likely to be asserted in relation to providing the information that proves highly relevant in the context of data reuse. For instance, providing thorough information on recipients (second, fourth, fifth, etc.) and data sources would typically require disproportionate efforts.

5.5.2. Enablers to data subjects' control

Paraphrasing Westin, effective control encompasses mechanisms that have two goals: helping individuals understand (1) *where* their personal information may flow and (2) *under what conditions* it may flow.[824] The right to information pursues both goals. To understand the location of data, controllers must communicate the details on recipients of data, international transfers of data, and data storage. To understand under what conditions the data flows, the GDPR informs users on the legal basis and the purpose of data processing. In the past, understanding of the flows may have been sufficient to achieve effective control. However, today's economic reality is more complex and disguised, and having control is more difficult. To address this issue, the GDPR has extended some existing provisions and introduced some new provisions intended to strengthen data subjects' control in the data-driven economy. These new mechanisms are, among others, the right to explanation and icons.

The so-called right to explanation was seemingly introduced in the GDPR to address the problem of incomprehensibility of data-driven decisions. Technical complexity of algorithmic decisions often makes it impossible to explain how exactly data was used. This is why the right to explanation encompasses not only a requirement of meaningful information but also information about the significance and consequences for an individual. This change is promising, although it does not come without problems, such as difficult implementation and limited scope.

The right to explanation is only the starting point of an EU journey towards a more comprehensive regulatory framework for AI. Within the GDPR, the new right to explanation is enhanced by some other relatively new overarching provisions on accountability, fairness, and transparency, and by more tangible requirements such as that on the privacy impact assessment. In addition, AI decisions will probably be tackled as a separate initiative on the EU level. It has been suggested that a general framework on algorithmic accountability and transparency could importantly strengthen consumers' rights. Liisa Jaakonsaari, an EU MP, recently proposed '*a general framework on algorithmic accountability and transparency*' that could be the next step in achieving these goals without raising unrealistic expectations regarding the right to information in the GDPR.[825] Furthermore, the EC just

[823] Article 14(5)(b) of the GDPR.
[824] Westin (2015) 5.
[825] Lisa Jaakonsaari, 'Who sets the agenda on algorithmic accountability?' *EURACTIV* (26 October 2016) <https://www.euractiv.com/section/digital/opinion/who-sets-the-agenda-on-algorithmic-accountability/> accessed 7 June 2018. Jaakonsaari also warns of the fact that the right to explanation only applies to a relatively narrow segment of algorithmic decision-making, as the definition of "solely automated" can be circumvented.

recently created the European Group on Ethics in Science and New Technologies, which has been entrusted with the task of examining the needs for the regulation of AI.[826]

Icons can be seen as another enabler in the sense that they bring an additional option for consumers who prefer visualisations, and that they replace complex privacy policies by a series of simple images. The introduction of icons and some related mechanisms[827] in the GDPR indicates a stronger link between data protection and consumer protection. In fact, the convergence between data protection and consumer law that has been increasingly discussed is something that also works to data subjects' benefit. After all, the failure of controllers to fulfil their information duty can have adverse legal consequences, a combination of those stemming from contract law and consumer protection law.[828] In recent investigations of information duties (typically in relation to privacy policies), the authorities have required changes based on both data protection and consumer protection law. For example, the Norwegian Consumer Ombudsman requested that the users of activity trackers such as Fitbit and Jawbone be notified of changes in privacy policies and other terms, to prevent users from suddenly finding themselves having implicitly 'agreed' to something of which they had no knowledge.[829] A policy that does not respect those requirements is deemed null or void, and as a consequence consumers have a complaint or class action.[830] The bond between data protection and consumer protection policy is meant to intensify in the future. For instance, the EU Commission's proposal of the directive on certain aspects concerning contracts for the supply of digital content is the first indicator of this new regulatory vision.[831]

5.6. Conclusions

This chapter sought to answer the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* While this research question refers to data subject rights as a whole, in this chapter the scope was narrowed down to the right to information.

In the first part of the chapter, the right to information was assessed in the context of the data-driven economy. It was shown that, in particular, the information about the legal basis for data processing, third parties involved in data processing, the source of personal data, and the information about purposes of data processing are what give data subjects the most relevant information about data processing. The GDPR extends the scope of the information catalogue available to data subjects and pays more attention to user-friendly design of the form in which the information is presented. Specifically, the right to explanation and icons seem to offer a new, promising option to exercise more control over modern data flows. In spite of these novel steps in the GDPR, entitlements that the law affords are undermined due to three groups of factors: psychological, technological, and economic. In the data-driven economy, these factors seem to gain influence and have a negative impact on data

[826] <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence> accessed 6 June 2018.
[827] Provisions on the quality of information in Article 12.
[828] Kuner (2012) 286.
[829] Forbrukerradet (n 755) 9. Cases in which both types of law overlap have already been considered by the CJEU; see for example Case C-191/15, *Verein für Konsumenteninformation v. Amazon EU* [2016] ECLI:EU:C:2016:612.
[830] Kuner (2012) 286.
[831] See more in Chapter 3.

subjects' ability to control information flows. The GDPR changes are not radical enough to revolutionise the impact of the right to information. However, this does not mean that the right is a paper tiger. After all, the right to information is not addressed to data subjects only, but establishes transparency for a whole economic environment including competitors, civil society, and regulators. Post-GDPR, national DPAs have become more active in terms of spotting inappropriate information practices. Finally, the right to information is not an isolated right but is part of a comprehensive data protection and a broader EU law regime. This regime may not excel in facilitating meaningful control for an individual, but it does certainly promise one of the most granular and comprehensive data protection mechanisms to date.

6. THE RIGHT OF ACCESS UNDER EU DATA PROTECTION LAW

6.1. Introduction

Contrary to the right to information, which aims to facilitate control in the stage *before* data processing starts, the right of access applies in *subsequent* stages of data processing.

The rationale for the right of access to personal data is similar to that for the right of access to governmental records.[832] Having access to information that is processed by 'data barons',[833] governments and commercial organisation alike, tends to meet two objectives: protecting the right to privacy and establishing a level playing field between data subjects and controllers. In the *Rijkerboer* case,[834] where the appellant requested access to information on the disclosure of his personal data to third parties, the CJEU established a strong link between the realisation of the right of access and the fundamental value of privacy: *'right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorized recipients. […] [I]n order to carry out the necessary checks, the data subject must have a right of access to the data relating to him […] .'*

The right of access, as one of the control entitlements, represents a key element in enhancing users' control over their personal data.[835] The right entitles a data subject to receive information on whether or not his personal data is being processed, and if so, to access his personal data including additional information about data processing (Article 15 of the GDPR). The objective of the right is to provide comprehensive access to data about an individual's use of a service, conveniently, securely, privately, and free of charge.[836] The right can be exercised offline and online, but the online manifestation is what mainly engages my interest in this chapter.

Access to personal data not only tends to engage individuals and enhance their informational self-determination as an aspect of the broader right to privacy: it also invites scrutiny of organisations' information practices, and helps expose potential misuses of data (such as data fabrication in medical research).[837] Thus, it simultaneously safeguards privacy and establishes power symmetry between data subjects and data controllers.[838]

---

[832] Also known as freedom of information. This is how the CJEU explained the difference between the freedom of information and the data protection right: "*The first is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents, and to promote good administrative practices. The second is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private life, in the handling of personal data."* C- 28/08, *Bavarian Lager* [2010] ECLI:EU:C:2010:378, para. 49.

[833] See the explanation in Section 4.1.

[834] *Rijkeboer*, C- 553/07 [2009] ECLI:EU:C:2009:29, para. 49.

[835] European Commission, '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' (2010) 7.

[836] Fischer-Hübner and others (2013) 133.

[837] Jeantine E Lunshof, George M Church and Barbara Prainsack, 'Raw Personal Data: Providing Access' (2014) 343 Science 373 LP. Also see Fischer-Hübner and others (2013) 133.

[838] The values underpinning the right to access are essentially the same as those that underpin the right to information. An interested reader should therefore also refer to Section 5.2.

As already mentioned, one of the outcomes of the EU data protection law reform has been modernisation of individual rights, with the objective of empowering the data subject by, *inter alia*, granting her some new prerogatives.[839] Although the right of access obviously falls in this group, the GDPR did not bring any major changes to the structure or scope of the right. Apart from the extended scope and some minor modifications, the set up from the directive has been maintained.

This does not mean that the right has proven to work flawlessly or that no improvement is possible. In fact, in the recent years access to personal data has become more difficult to exercise. In complex modern economic environments with uncountable and/or undetectable flows of data and indefinite forms of secondary usage,[840] invoking the right is cumbersome, slow, and often incomplete.[841] Furthermore, access in the sense of empowering consumers has been hindered by a number of applications for technical (e.g. Skyscanner),[842] commercial (e.g. social media networks such as Facebook),[843] or ethical reasons (e.g. genetics data in research).[844] The transposition of the right has varied across the member states and its implementation has rarely exceeded the boundaries of mere compliance.[845] Tene and Polonetsky rightly observe that the right of access has remained woefully underutilised.[846] Considering the lack of any revolutionary change with respect to the right of access in the GDPR, their statement appears to be valid. As is shown in the following sections, in the age of data-driven technologies, applying the right in a manner and to the degree that would satisfy the modern regulatory vision of strengthened data subject control seems to be a utopian scenario.

Nonetheless, consumers have not ceased to seek answers to daunting questions such as what kind of data is processed and how, when, and where it is shared or sold.[847] In fact, some cases suggest that the right of access can be made operable if individuals are given the ability to handle their personal data in a tangible way. A successful example is online access to one's banking information, where consumers are given viable ways to both control and benefit from data processing.[848]

This chapter continues answering the fourth research sub-question which reads: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* While the

---

[839] Viviane Reding, 'Your data, your rights: Safeguarding your privacy in a connected world; speech for Privacy Platform "The Review of the EU Data Protection Framework" in Brussels, 16 March 2011' <http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm> accessed 7 June 2018.

[840] See the explanation of a data value chain in Chapter 2, section 2.3. Also see Helen Nissenbaum, 'Privacy as Contextual Integrity' [2004] Washington Law Review 119; Julie E Cohen, 'Law for the Platform Economy' (2017) 35 U.C. Davis Law Review 133.

[841] Fischer-Hübner and others (2013) 133.

[842] See section 6.3.1.

[843] See section 6.2.1.

[844] See section 6.2.2.2.

[845] Michael Veale, 'Ignore Mark Zuckerberg' *Slate* (12 April 2018) <https://slate.com/technology/2018/04/mark-zuckerbergs-misleading-promise-that-eu-privacy-rules-will-apply-to-american-facebook-users.html> accessed 7 June 2018.

[846] Tene and Polonetsky (2013) 263.

[847] Anca D Chirita, 'The Rise of Big Data and the Loss of Privacy' in M Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer 2018) 13. A good example of a persistent and privacy advocating consumer is Max Schrems, whose complaint resulted in the landmark case on safe harbour.

[848] European Data Protection Supervisor, 'Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability (Opinion 7/2015)' 12.

previous chapter analysed the sub-questions in the light of the right to information, Chapter 6 approaches it from the perspective of the right of access.

To this end, the chapter first discusses the normative scope of the right, and describes the regulatory framework of the right of access under the GDPR through the lens of the data-driven economy (section 6.2.1.). Subsequently, it analyses three specific situations of application (section 6.2.2.), explains some statutory limitations to access requests (6.3.) and illustrates how the right works in practice (section 6.4.). Finally, sections 6.5. provides some answers to the research question of how effective the right of access is in providing individual control over personal data. Section 6.6. then concludes the chapter.

6.2. The right of access under the GDPR

6.2.1. The right of access under the GDPR

The provision on the right of access in Article 15 can be broken down into three entitlements. First, it grants the right to a data subject to receive information on whether or not her personal data is being processed. Second, it allows her to be informed about the nature of the data processing. This additional information must be given in an intelligible form and needs to include purposes of processing, the categories of data concerned, the recipients or categories of recipients to whom the data are disclosed, the storage period,[849] the existence of some other rights, information about the source if the data was not collected from the data subject, and any available information about the source and logic involved in any automatic processing of data (Article 15, para 1, points (a) to (h)).[850] Finally and most importantly, the right allows a data subject to gain access to his personal data by receiving a copy of the data undergoing processing (Article 15, para 3).

The right of an individual to receive confirmation that information relating to her is being processed is generally understood to mean that controllers are required to respond to every request, even if the response is to deny that data is being processed.[851] The right of access gives individuals an option to check whether the entity has been processing their data. This is an important point in the data-driven economy considering the widely spread practice of data sharing and reusing which muddles consumers' understanding of their data location and flows. For example, some people are not Facebook members but nevertheless make use of Facebook's public pages or 'like' plug-ins when they surf other websites. Facebook also processes these persons' personal data (IP addresses) of.[852] As a consequence, the social network may process such data to target consumers with advertisements adapted to their personal preferences inferred from the pattern of their likes and websites' visits.[853] The right of access should allow also non-registered users to inspect whether and in what way their personal data has been processed.[854] This would strengthen data subjects' control and make access

[849] Or at least the criteria used to determine the period.
[850] See section 5.3.1. for more detail on what specific information means.
[851] Ustaran and International Association of Privacy Professionals (2012) 127.
[852] The so called shadow profiles; see for instance Gennie Gebhart, 'Facebook, This is not what "complete user control" looks like' (*Electronic Fontier Foundation*, 11 April 2018) <https://www.eff.org/deeplinks/2018/04/facebook-not-what-complete-user-control-looks> accessed 7 June 2018.
[853] 'Facebook wins appeal on Belgian tracking' *BBC* (30 June 2016) <https://www.bbc.com/news/technology-36671941> accessed 6 June 2018.
[854] Settings on the Facebook platform currently do not allow for such access.

rights more effective because it would no longer wrongly limit access to regular users of the service. However, as the next sections show, the implementation may be challenging.

In comparison to the data protection directive, the information to which the data subject is entitled under the GDPR's right of access is somehow broader, including the reference to the supervisory authority, information about control rights, and information about the third-party source of information. The latter in particular seems to be a consequence of the new economic realities, where more and more information is collected not from the data subject himself but through intermediaries and other third parties. In addition, the provision regarding the information about automated decision-making has been extended to include information on significance and possible consequences of data processing for a data subject.

One piece of information that is not within the scope of the access right is information about a legal basis. Is there any good reason for excluding this? During the negotiations for the GDPR, the Hungarian representatives in the Council suggested adding it to the information catalogue, but their proposal was not accepted. It is certain that the information on legal basis is not irrelevant. Consider the Cambridge Analytica and Facebook scandal: Facebook collected users' data based on their consent. At a later point in time, this data was shared with a third-party app on the basis of a public (research) interest. This legal basis proved to be illegal, since the final use of data was commercial rather than scientific.[855] However, it is unlikely that accessing the information on legal basis would be of much use to data subjects. While it is true that this information could shed light on possibly problematic uses of data, it is unlikely that data subjects could effectively monitor the use of data in such a way. Moreover, Facebook recently revealed that it was cooperating with over 90 million third-party apps.[856] Providing this information would represent a large, maybe even disproportional burden for data controllers.

In principle, the right of access provides data subjects with a broad range of information and as such should give them more control. However, there are a few limitations to applying the right to its full effect. In the data-intensive online economic environment, providing a copy of personal data can be challenging for several reasons. First, the right of access does not apply to data on the aggregated (anonymised) level, although the latter is largely used in the data economy and may have consequences for individuals. Second, data is often combined and/or is a shared resource. Both facts complicate the application of the right of access. Finally, the right of access can be used to monitor algorithmic decisions, but the extent to which this can be done is disputable. In the following three sections, all these issues are explained in more detail.

---

[855] Carole Cadwalladr and Emma Graham-Harrison, 'How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool' *The Guardian* (17 March 2018) <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-
analytica-kogan-data-algorithm> accessed 5 June 2018.

[856] Brittany Darwell, 'Facebook platform supports more than 42 million pages and 9 million apps' *Adweek.com* (27 April 2012) <http://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/> accessed 22 may 2018.

6.2.2. Examples of specific applications of right of access

6.2.2.1. The right of access on a continuum between personal and anonymised data

According to Article 15, a data subject can access her *personal* data. This means that before granting access, the controller has to clarify whether the requested data actually falls under the definition of personal data. Determining the exact scope of the right has been difficult due to the blurred boundaries of the scope of personal data.[857]

For reasons of security and convenience, data-driven companies typically use anonymised or pseudonymised data.[858] Anonymised data is considered non-personal data because identifiers that could lead to a person have been removed from the data set. Data protection law is focused on identified or identifiable individuals, therefore in case of anonymised data it no longer applies. The same goes for the right of access, meaning an individual cannot inspect his data after identifiers have been removed.

However, anonymisation of data is not always a solution for privacy. In fact, anonymised datasets may often be as useful as personal data and may have similarly (negative) consequences for someone's privacy. Although the identity of users is effectively protected when every dataset is taken independently, certain individuals could nonetheless be re-identified by aggregating data coming from multiple data sources into one large dataset so as to find new patterns and correlations.[859] In other words, it is becoming increasingly easy to de-anonymise data.[860] By developing algorithms capable of turning anonymous data back into names and addresses, computer scientists have proven that anonymisation techniques may fail.[861] This does not mean that the practice of anonymising data should be abandoned, but it is a good reminder that anonymisation is indeed an imperfect privacy-preserving

---

[857] In *Y.S.*, the question of personal data scope was critical to determine whether data subject could access some specific documentation or not. In the judgement, the CJEU was quite restrictive in terms of personal data definition. Following AG's opinion, it held that mere legal analysis of an asylum-seeking status is not personal data. On these grounds, the asylum seeker was denied the possibility to inspect his file to the extent that it related to the legal assessment of his/her legal status. One possible reason for the CJEU strict stance might have been the attempt to scold down the number of (unsubstantiated) data subject requests. However, that view could be problematic if the decision was applied in a data-driven environment. For instance, the assessment of credit rating could be compared to a legal analysis of someone's personal situation.[857] Instead of applying legal rules on someone's data, data is assessed by an algorithm using selected metrics. The result of the assessment is a decision that is likely to influence data subjects. It does not seem convincible that such analysis would escape the right to access. In addition, while laws that apply to certain facts are publicly available, algorithms are not, which makes access to the information on of the metrics even more pressing. In the GDPR, automated decision-making is specifically listed as one of the types of information that can be accessed by a data subject. For similar considerations see also: E Brouwer and F Borgesius Zuiderveen, 'Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. and M. and S. judgment (C-141/12 and C-372/12), case report' European Journal of Migration and Law 17 (2015) 268. Another judgement in which the Court dealt with the boundaries of personal data in relation to the right of access was C-434/16, *Nowak* [2017] ECLI:EU:C:2017:994.

[858] *'… consumer mistrust of e-commerce firms offering their own dubious "guarantees" of anonymization, thereby reinforcing the "privacy is dead" meme" …'* The anonymization debate should be about risk, not perfection. Woodrow Hartzog and Ira Rubinstein, 'The Anonymization Debate Should Be About Risk, Not Perfection' (2017) 60 Communications of the ACM 22.

[859] Primavera De Filippi, 'Big Data, Big Responsibilities' (2014) 3 Internet Policy Review 4. Combining databases, a regular business in the data-driven economy, can lead to de-identification of almost any aggregated database. Purtova rightfully commented that in the EU even weather data can be personal. Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law' (2018) 10 Law, Innovation and Technology.

[860] Ohm (2010).

[861] Narayanan A and Shmatikov V, 'De-Anonymizing Social Networks' (2009) 30th IEEE Symposium on Security and Privacy, 2009.

technique.[862] Furthermore, negative consequences may go beyond privacy intrusions. Consider the following case: based on aggregated information on Quran purchases, the police may determine in which neighbourhoods more policemen should be present. Although this is a decision on a group level, taken, in principle, without the use of sensitive data, it may affect individual citizens and lead to discrimination and surveillance. However, as only anonymised data was used to impose the measure, individuals are not able to inspect the dataset under the right of access.

As Zwenne indicates, such data is excluded from the scope of data protection law for a reason. Stretching the definition of personal data may lead to serious (practical) problems: '*if, for example, someone wants to make use of his or her subject access rights, the controller has to establish the identity of the one requesting access. This will be difficult - if not downright impossible - when it concerns access to data about individuals whose identity is unknown.*'[863]

While Zwenne's point should be endorsed, the answer is less straightforward when it relates to data that falls in the area between anonymised and personal data. This grey area concerns data from which certain identifiers are removed so that it no longer can be attributed to a data subject.[864] For instance, today, online services are able to use unique identifiers to track individuals while not being able to identify the user.[865] This typically occurs as part of online targeted advertising.[866] Should an individual know that she received an ad because the analysis of her profile pointed out a personal characteristic?[867] The Article 29 Working Party thinks she should, as every time data is used to single someone out, this should be deemed personal data processing.[868] Such an interpretation is also in line with the GDPR's views on profiling, where any type of data use that includes personal information to predict someone's preferences is considered personal data processing.[869]

Data that is processed in a way that it can no longer be attributed to an identifiable or identified individual is referred to as pseudonymised data.[870] Does the right of access apply to such data? Article 11 (paragraph 2) of the GDPR tries to resolve the conundrum: *'if the controller is able to demonstrate that it is not in a position to identify the data subject, […] Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.'* Thus, under Article 11, the right of access should be granted in this situation if a data subject, for the purpose of exercising his rights under Articles 15 to 20, provides additional information enabling his or her identification. At first glance, the solution seems balanced. However, for the reasons above, its practical application may prove difficult. First, requesting

---

[862] Ohm (2010).
[863] Zwenne (2013) 9.
[864] For the analyis of different categories of non-personal data underthe GDPR, see Runshan Hu and others, 'Bridging Policy, Regulation and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017).
[865] Comments of the LIBE Committee to the proposed GDPR, Article 10 on page 82/218. *Supra* n 662.
[866] Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data - a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2017) 34 Wisconsin International Law Review 285.
[867] Josh Constine, 'Facebook Finally Lets Its Firehose Be Tapped For Marketing Insights Thanks To DataSift' *TechCrunch* (Mar 10, 2015) <https://techcrunch.com/2015/03/10/facebook-topic-data/> accessed 8 June 2018.
[868] Zuiderveen Borgesius (2016) 31. Also see Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data'. However, note that the CJEU did not adopt the Article 29 Working Party's test when determining what is personal data in the Breyer case (C-582/14, *Breyer* [2016] ECLI:EU:C:2016:779). Bird & Bird (2017) 5.
[869] GDPR, Article 4.
[870] GDPR, Article 4(5).

that individuals establish proof of personal data may be a substantial burden given their lack of expertise and the platforms' powerful role. Cohen observes that consumers' personal data is often embedded deeply within the operating protocols of a mobile phone platform or web browser, and may involve complex commercial relationships among multiple players in platforms' cross-licensing ecologies. Platforms are leading the way: '*That complexity and opacity of the platform firms suggests that traditional methods proposed for ascertaining personal data do not fit the fragile balance between the powerful platforms and powerless users*.'[871]

6.2.2.2. Accessing shared data and coupled databases

Two distinct characteristics of data make it difficult to apply Article 15 in its entirety: first, data is a *shared resource,* and second, it is *often combined*.

With regard to the first point, accessing data on one person might infringe the privacy of another person. Given recent advances in data processing techniques, personal data is no longer strictly personal. For example, consider genetic data. An individual DNA sequence also reveals information about other people sharing the same genes. Personal data disclosed by one individual – when put through the big data algorithms – reveals information about and hence presents benefits and risks to others.[872] Paragraph 4 of Article 15 contains a safeguard that the execution of the right of access should not adversely affect the rights of others.[873] Yet sometimes, like in the given example of DNA data, the opposing interests of two or more persons are impossible to reconcile. A similar situation occurs when accessing social media data: a list of one user's contacts also includes a broad range of information about profiles and online activity of those contacts.

Second, in the course of processing, data is often transferred to and reused by third parties. The GDPR requires that the controller inform individuals about those recipients, but it is not the controller's job to facilitate access to this information. Rather, data subjects should turn to the secondary data controllers with a new request.[874] It is important, however, that primary controllers allow access to third-party information which has been coupled with their own data and is still being used on their premises. For example, in its privacy policy, LinkedIn states that data flowing from data aggregators is coupled with LinkedIn's own data and used for advertising purposes.[875] However, the access request to LinkedIn only results in receiving a limited set of information without any hints of how data is

---

[871] Cohen, 'Law for the Platform Economy' 37.

[872] 'Data Management and Use: Case Studies of Technologies and Governance (Produced for the British Academy and the Royal Society)' (2017) 28 <https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-case-studies.pdf>. One case concerned the identification of a particular gene in a boy who presented with autism, which was deemed to have little immediate clinical use for the macnagement of the boy but potential clinical use for the management of the family.

[873] See also recital 63 of the GDPR.

[874] This situation should not be confused for the situation in which controller has authorized a *processor* to analyze the information. In such relationship, data subjects still have the right to request access directly form the controller. The ICO gives the example in the employment context: "*An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party data processor is analysing the information. The employer receives a subject access request from a member of staff. To respond, the employer needs information held by the data processor. The employer is the data controller for this information and should instruct the data processor to retrieve any personal data that relates to the member of staff."* UK Information Commissioner Office, 'Subject Access Code of Practice' 21 <https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf> accessed 8 June 2018.

[875] LinkedIn's privacy policy <https://www.linkedin.com/legal/privacy-policy> accessed 7 June 2018.

combined and in what way a user's profile has been improved.[876] As these practices are indeed at the core of LinkedIn's commercial strategy, it would be just for an individual to gain some insight into the mechanism of profit generation by processing his personal data.

The examples above show how specific characteristics of data result in restricted effectiveness of the right of access. When a data set includes information on third persons, access can be restricted or denied. Similarly, once data has been shared or reused with third parties, access to it becomes more difficult or even impossible. As the GDPR did not change the basic design of the right of access, in the future the right may suffer from the inability to address changes in the data economy in which processing is becoming increasingly complex and uncontrollable.

6.2.2.3. Access to information on automated decision-making

Although the DPD version of the right of access was carried over to the GDPR without any major changes, in one aspect its scope extended. Article 15 states that the response to an access request should also provide information on logic and the envisioned consequences and significance of automated decision-making. This addition, which echos the right to explanation in Articles 13 and 14 of the GDPR, fell outside the scope of the DPD. The tiny change is in fact highly significant. Veale and Edwards claim that precisely this extra piece of information is the GDPR's strongest weapon against non-transparent data-driven practices in relation to algorithms.[877] Namely, in the new economic environment there is a high need for more transparency of automated decision-making as now even mundane activities involve complex computerised decisions: everything from cars to home appliances now regularly execute computer code as part of their normal operations.[878] An illustrative example of automated decision-making is price discrimination used by airlines to set ticket prices. The views on whether users' profiles are decisive in setting the price vary, but dynamic pricing typically takes into account some personal information. Since air travel has become a critical means of transport for many of us, knowing how the price is determined is certainly valid, important information. Yet, how exactly our personal information is used to determine ticket prices is largely blurred. For example, some people have observed that their ticket suddenly changed when they deleted cookies or used a VPN connection on their computer. This suggests that the information about the (location of the) computer used by a visitor to surf the website could drive the price up or down.[879,880] The benefit of the new provision in Article 15 in such cases is that it would allow a data subject access to not only meaningful information about the logic that is behind the determination of the ticket price, but also to the information on significance and consequences for the final price. Thus, through the exercise of this right, the data subject can become aware of a decision made, including one based on profiling her.

However, accessing such data including the explanation will only be possible as long as the buyer's personal data is included among the factors that are built into the algorithm.[881] If the company

---

[876] Information based on a personal access request sent in June 2017.
[877] Lilian Edwards and Michael Veale (2017) 24.
[878] Kroll and others (2016) 1.
[879] 'Save Money on Flights: How We Found $400+ in Savings on Plane Tickets' (*Safer VPN blog*, May 16, 2017) <https://www.safervpn.com/blog/save-money-on-flight-tickets-vpn/>.
[880] Some other research found that no special correlation could be drawn between the price and personal data (i.e. cookies). Thomas Vissers and others, 'Crying Wolf ? On the Price Discrimination of Online Airline Tickets' (2014) <https://hal.inria.fr/hal-01081034/document> accessed 7 June 2018.
[881] Borgesius and Poort (2017) 14.

calculates the score without the use of personal data, the access right cannot be applied. Does this mean that price discrimination is out of the question? Not necessarily. Researchers showed that Amazon had managed to discriminate against online shoppers based on their laptop type (offering higher prices to those who used MacBooks) without including any piece of personally identifiable data.[882] Although such data processing might have violated individual rights,[883] the right of access cannot be exercised as a tool to inspect data (re)use.

One more question is important in relation to the right to explanation within the framework of the right of access: could the right be used to request explanation of individual decisions that have already been made based on personal data, or should it be limited to providing a description of some basic functionalities of the system?[884] An important point to note is that requests for access under Article 15 typically come after data processing has already taken place. Therefore, it could be argued that the data controller is required to provide *ex post* tailored knowledge about specific decisions that have been made in relation to a particular data subject.[885] Such a solution appears sensible and seems to promise an *ex post* right to an explanation, despite some textual quibbles.[886] Wachter et al., however, claim that the right of access could not be stretched that far and argue that the wording of the article is too narrow to construct any sort of entitlement that could equal the right to explanation.[887] By using language analysis and national case law, they established that the right to explanation was not what lawmakers had in mind when drafting Article 15.[888] While the authors aknowledge that some sort of a right to explanation could be derived from the safeguards described in Article 22(3) of the GDPR, they emphasize that the scope of the article is limited as it only applies to a narrow range of decisions that are 'solely based on automated processing' and with 'legal' or 'similarly significant' effects for the data subject.[889] The Article 29 Working Party appears to align itself with Wachter et al.'s view, agreeing that the right of access only provides a 'more general form of oversight', rather than 'a right to an explanation of *a particular* decision'.[890]

Given the pressing need to address the question of algorithmic accountability, *a priori* rejecting the idea of the right to explanation of *a particular* decision should not be endorsed.[891] The reference to national sources is a weak argument, considering the novel and supra-national nature of the GDPR.[892] Furthermore, the right is already limited by the fact that non-personal data falls outside its scope, regardless of how useful this data can be in determining people's preferences and weakest points.

---

[882] Philip Hacker and Bilyana Petkova, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers' (2017) 15 Northwestern Journal of Technology and Intellectual Property 1, 13.
[883] See section 2.4.2.4.
[884] In the sense of what the system is capable of.
[885] Lilian Edwards and Michael Veale (2017) 34.
[886] Ibid.
[887] Wachter, Mittelstadt and Floridi (2017) 5.
[888] Ibid., 22 and the following.
[889] See section 9.3.3.3. for more detail on this alternative route to the right to explanation.
[890] Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398, 399.
[891] Andrew Burt, 'Is there a right to explanation for machine learning in the GDPR' *IAPP (1 June 2017)* <https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/> accessed 8 June 2018.
[892] Compare to the CJEU's views in Google Spain, where the court did not hesitate to adopt its own interpretation of the Data Protection Directive. Some authors point out that some influence of the constitutional traditions of member states are indeed played a role in establishing the data protection right as the basis of the EU data protection regime but the regime nonetheless maintains its inherently supranational character. Yvonne McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017).

Considering the cases where lack of algorithmic accountability led to unwanted consequences, a broader interpretation seems more appropriate.[893, 894]

Even if the suggested broad interpretation becomes a reality, some questions will nevertheless remain open. The following one is particularly important: How could the explanation of algorithms under the right of access be done in practice, or in other words, what would the procedural steps to access the information on algorithms involve?[895]

6.3. Regulatory boundaries of data subjects' data requests

6.3.1. Limitations regarding the cost, frequency, and scope of requests

The DPD allowed for national legislations to define the meaning of 'reasonable intervals' and 'without excessive delay or expense'. This resulted in variations across member states.[896] For example, in Ireland, requesting access can cost a maximum of 6.35 EUR,[897] while in the UK this is almost twice as much (£10).[898] Under the GDPR, regulatory freedom of member states in the area of personal data protection is restricted. The first copy of data should be free of charge and further copies can cost a reasonable fee (Article 15(3)). Although the fees under the DPD were not high either,[899] they might have discouraged individuals from invoking the right. It is thus reasonable to expect that the GDPR's lenient approach with regard to the fees will work as an incentive to individuals willing to seek access.

It is surprising that despite being tech-savvy, some companies still approach the requests for access in a traditional manner. Skyscanner, a travel fare aggregator website and travel meta search engine, requires users to submit requests in writing to their UK-based legal office.[900] Considering the cost and the time needed to print out a letter and take it to the post office, regular mail is a highly unattractive option to process data subject access requests. In fact, such a long-lasting procedure may discourage individuals from even trying to seek access. Under the GDPR, remote access is the default option, especially for data-driven companies. Article 15(3) states that data subjects can make requests by electronic means, and that in principle the information shall be provided in a commonly used electronic form. Recital 65 of the GDPR offers some implementation guidelines: *'Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.'* As personal information is increasingly being processed online

[893] See for example: Aylin Caliskan, Joanna J Bryson and Arvind Narayanan, 'Semantics Derived Automatically from Language Corpora Contain Human-like Biases' (2017) 356 Science 183 LP.
[894] In crafting out the boundaries of the entitlement, some guidance could be provided by the Article 29 Working Party and/or the future EU data protection board. So far, the Working Party has already clarified some other data subject rights such as data portability and the right to be forgotten. A general EU guidance document would lead to a more harmonized application of the right and would decrease uncertainties. See for example Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' [2017] April <http://ec.europa.eu/justice/data-protection/index_en.htm>.
[895] For some ideas see Chapter 9, Section 9.3.3.3.2.
[896] Ustaran and International Association of Privacy Professionals (2012) 126.
[897] See the guidance on the right to access by the Irish DPA <https://www.dataprotection.ie/docs/Accessing-Your-Personal-Information/r/14.htm> accessed 8 June 2018.
[898] UK Information Commissioner Office, 'Subject Access Code of Practice' 7.
[899] Due to the requirement of "reasonable" fee in Article 15(3).
[900] Skyscanner's privacy policy (version available in 2017) <https://www.skyscanner.net/privacypolicy.aspx> accessed 15 July 2017.

and/or in a digital form, this is a sound requirement. In fact, when a data-driven organisation implements a non-digital type of access procedure, users may call out its hypocrisy.

How far in the past does the right of access extend? In *Rijkerboer,* the applicant demanded access to information on all disclosures of his personal data to third parties from the previous years.[901] However, under the Dutch law, his right was limited to one year back in time. To further complicate things, the requested data had already been erased in accordance with the principle of storage limitation. In the judgement, the CJEU weighed the interest of data subjects of access against the burden imposed on data controllers to ensure that personal data is available to data subjects (Article 6(1)(e)). The court ruled that limiting the data on recipients does not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller: '*to ensure the practical effect of the provisions on the right to access, that right must of necessity relate to the past. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered.'* The court noted that while data related to transfers was deleted, basic personal data remained stored for a much longer period. This mismatch (or even hypocrisy) was considered the decisive element to argue that storing the other data for the same period would not constitute an excessive burden for the controller.[902,903]

The need to find a balance between the interests of data subjects who want access and the interests of data controllers who want data security by making less data available will likely increase in the future. Researchers have shown that many new technologies such as Apple's Siri voice assistant and Transport for London's Wi-Fi analytics require difficult trade-offs.[904] Specifically, some privacy by design techniques that tend to eliminate availability and prevent identifiability of personal data may be in conflict with the right of access and other data subject rights.[905]

Finally, it seems plausible that the right of access could be limited when requests are fraudulent. Privacy experts working in the practice have warned of the intention of some would-be litigants to use the right to obtain pre-action disclosure of documents to gain an advantage in litigation or complaints against third parties. As it can be difficult to obtain evidence of the true motive for the access request, the right of access may lead to abuse.[906] Interestingly, in the UK this trend started only after the courts

---

[901] C- 553/07, *Rijkeboer* [2009] ECLI:EU:C:2009:29, para. 49.

[902] The UK data protection act does not define 'disproportionate effort', but the courts have explained that there is scope for assessing whether, in the circumstances of a particular case, complying with a request by supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's right of access to their personal data. UK Information Commissioner Office, 'Subject Access Code of Practice' 45. Also see Anya Proops, 'Yet another subject access judgement ...' (*Panopticon blog*, 6 March 2017) <https://panopticonblog.com/2017/03/06/yet-another-subject-access-judgment/> accessed 8 June 2018.

[903] The court seemed to disregard the fact that limited storage period also aimed to protect individual right not only to decrease controllers' burden.

[904] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) forthcoming International Data Privacy Law.

[905] Compare with section 6.1.2.1.

[906] For a similar discussion see also Andrew Evans, 'Subject Access Requests: Fishing for Information?' <http://gateleyplc.com/wp-content/uploads/2016/01/Subject-Access-Requests-fishing-for-information.pdf> accessed 8 June 2018.

had adopted a wider definition of personal data.[907] The Slovenian information commissioner pointed to the same problem, acknowledging the lack of any viable mechanism to prevent abuses.[908]

As a matter of fact, a data controller can do little to prevent abuses of the right of access. In principle, she can neither examine the intentions of those that request access nor block access because of inappropriate intentions.[909] Only under strict conditions might it be possible to reject those requests that are fraudulent *prima facie*.[910] Under the UK law, access to information which is likely to prejudice the carrying out of social work because of the risk of serious harm to the physical or mental health or condition of the requester should be subject to an exception.[911] In an identical situation, the GDPR would probably lead to the same conclusion as it foresees an exception to the right of access to safeguard general public interest such as public health and social security (Article 23 (d)). Another route to limit fraudulent access requests would be via Article 12(5), which prohibits requests that would adversly affect the rights and freedoms of others.

At this point, the reader should refer back to the discussion on the changed balance between users and controllers in the data-driven economy.[912] Regarding the abuse of the right, the specific interaction between data-driven organisational forms and their users should be distinguished. It is difficult to envision a situation in which a platform such as Facebook, where requests for data access are managed automatically, could claim a misuse of the right of access. Furthermore, data subjects are apparently in an unfavourable position towards the platforms, which makes the abuse even less likely. While traditional businesses might well face trouble if they received an excessive number of requests, this is less unlikely to happen in the case of some modern organisational forms.

6.3.2. Further exceptions

Exceptions and limitations to the right of access can be roughly divided into two groups. Those in the first group pertain specifically to the right of access, such as limitations regarding the frequency of requests or the need to protect the privacy of third parties.[913] Limitations belonging to this group were described above. The second group includes general exceptions that apply to the entire catalogue of control rights (Article 23). For instance, access to certain data can be limited for reasons of public security or protection of professional ethics.

6.4. How the right of access works in practice

Max Schrems' story about accessing his personal information processed by Facebook is one of the few data access requests that went viral. Schrems' experience is interesting because Facebook is a typical representative of the 'big data barons'. After requesting access to the data, then held at Facebook's US

[907] That is aligned with the EU definition.
[908] The client of a bank who has been in the relation with the bank for a few years requested the bank for the personal data on him. The DPA wondered whether this request went too far and whether it could be considered a misuse of the right. Urban Brulc, 'Do kod seže pravica seznanitve z lastnimi osebnimi podatki?' [2016] Pravna praksa 6.
[909] Ibid.
[910] Ibid. Possible criteria to assess the abuse could be: how explicit the abuse of the right was, if the abuse was objective, if it was executed with conscience, if the purpose was to inflict harm etc.
[911] UK Information Commissioner Office, 'Subject Access Code of Practice' 56.
[912] See Chapter 2.
[913] German law expressly provides that the information should not be disclosed when the interest of a trade secret protection outweighs the interests of a data subject. Ustaran and International Association of Privacy Professionals (2012) 127.

servers, Schrems received a file containing over 1,200 pages about the data that had been processed about him.[914] While the overload of information could be seen as camouflaging meaningful data, it also indicated the struggle of data controllers to appropriately address individual access requests. To help data personal data controllers, in 2016 the UK information commissioner issued useful guidance on how to appropriately react to data subject requests.[915]

Today, Facebook enables a more user-friendly experience. Within its Settings function, a user can easily and speedily download her data.[916] Compared to Schrems' experience, this electronic copy of users' data seems somehow inadequate and scarce.[917] For example, the history of Facebook messages is presented in a chaotic way. Since some messages seem to have been left out, more information about the basis on which the data was brought together would be welcome. No such explanation is provided. Rather, it looks like Facebook assembled the information for the mere sake of meeting compliance requirements. The only information that exceeds what is available on each person's online profile is the data regarding individuals' preferences and interests used to determine interaction with advertisers. Characteristics of a person's profile are listed as bullet points. However, no explanation is given concerning the way this information is actually applied.[918] Examining the GDPR's text, it would be possible to argue that any additional explanation should be part of the controller's response to the request. After all, the GDPR text contains the provision that explicitly demands that information regarding data access be provided in an *'intelligible and easily accessible form, using clear and plain language*'.

Other websites perform even worse in this respect. Skyscanner, for instance, requires users to approach its UK legal office in writing and does not provide any user-friendly interface. Acxiom, the world's largest data broker, only provides data if the individual pays for access.[919] However, even those who agree to pay are not necessarily provided with access to all of the data that Acxiom has associated with them and/or all of the inferences made from that data.[920] As the FTC's report points out, data brokers typically provide access to raw data and not to the proprietary information that they derive through algorithms.[921] As a result, consumers may not know that they have been categorised in a particular manner.[922] Such a limited response is not entirely in line with the new version of the GDPR, particularly not with the explicit reference to automated decision-making in Article 14 (para 1, point (h)).

However, some technical or/and organisational solutions that tie data access to a commercial service have proven successful. Cathy O'Neil writes about a positive experience with open data access in the US. From 1985 to 2013, the cost of academic education at the US universities skyrocketed: the increase during that period was almost 500%. To a large degree, the problem was associated with the deployment of a non-transparent algorithmic ranking program which prioritised programs with higher

---

[914] Kashmir Hill, 'Max Schrems: The Austrian Thorn In Facebook's Side' *Forbes* (7 February 2012) <http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/> accessed 23 January 2016.
[915] UK Information Commissioner Office, 'Subject Access Code of Practice' 56.
[916] Personal request made in June 2017.
[917] Ibid.
[918] See Article 12 (1).
[919] This might be legal in the US but not under the GDPR provisions.
[920] Federal Trade Commission, 'Data Brokers - A Call for Transparency and Accountabilty' (2014) vi.
[921] Ibid.
[922] Ibid.

tuition fees. The US government mitigated the problem of the black box by replacing rankings with data released and open to everyone's access on its website. Today, students may ask their own questions about the things that matter to them—including class size, graduation rates, and the average debt held by graduating students. They do not need to know anything about statistics or the weighting of variables. O'Neil notes: *'The software itself, much like an online travel site, creates individual models for each person. Think of it: transparent, controlled by the user, and personal*.'[923] Another example of successfully implemented data access which is tied to a commercial service is access to online banking information.[924]

The recent technological developments indicate that the right of access may transform in the future. Blockchain, which is a distributed database used to maintain a continuously growing list of records, called *blocks*, could allow data subjects and trusted persons (e.g. doctors) easy, secure, and real-time access to personal data.[925] Blockchain would document someone's transactions or actions (e.g., visits to the doctor) and these records would be open access. However, as not only data subjects but also everyone else involved in the blockchain could access this same information, this could raise some other privacy issues.[926] Blockchain is still in its early stages of development and only time will tell whether it could be a feasible solution for the right of access.

6.5. The right of access as a control affording entitlement

Building on the findings from the previous sections, this section summarises some key barriers to providing access. Next, it turns to those aspects of the right of access which prove more enabling. The aim is to assess whether the right is overall successful in helping data subjects exercise control over their personal information.

6.5.1. Limits to data subjects' control

Despite all the undeniable benefits of someone's access and scrutiny over data, the right of access remains ineffective. This ineffectiveness has technological, economic and psychological causes.

Many of the reasons for ineffectiveness stem from the new realities in the data-driven economy: data's specific nature as a shared resource, use of anonymised data which falls outside the scope of data protection law, and the outspread reuse of data and combinations. In addition, the data economy is increasingly an economy of platforms.[927] The specific nature of platforms – opaque, two-sided, and highly technological – adds to the problem. Platforms are growing increasingly powerful and almost untouchable (to borrow Cohen's words). In such an environment, access rights often become ineffective.

---

[923] O'Neil (2016) 67.
[924] European Data Protection Supervisor, 'Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability (Opinion 7/2015)' 12. This successful implementation of the right to access is limited to a specific dataset which might be the reason for its successful implementation as opposed to a more complex data sources handled by social media companies.
[925] Molteni Megan, 'Moving pateint data is messy but blockchain is here to help' *Wired* (1 February 2017) <https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/> accessed 8 June 2018.
[926] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) 23.
[927] See Cohen claiming that platforms are not merely a business model but an organizational form in the new economy. Cohen, 'Law for the Platform Economy' 2.

The right of access granted to individuals under the data protection directive was implemented narrowly.[928] Organisations provided individuals with little useful information but nevertheless complied with the law.[929] People were given access to only some of the digital data that they generated, with the vast majority of it unavailable to them because it was in the possession of Internet companies.[930] This trend may continue in the era of the GDPR, as the DPD's version of the right of access has mostly been carried over.

Furthermore, the analysis of both the right to information and the right of access have shown that people may experience technical difficulties in understanding digital data, visualising it, or seeing ways of making data work for them. Moreover, they may have difficulties accessing their own data. An additional trouble is that individuals often lack the time or interest to 'indulge in transparency and access for their own sake'.[931] As a result, only few of them exercise these rights in practice.

In conclusion, granting access also leads to some risks. Blockchain is a distinct example of a technology which presents an ideal setting for data access but is at the same time flawed because on a blockchain, access can never be exclusively afforded to a data subject. Some other modern web-based information and communication technologies that render direct data access more technically feasible and economically affordable, thus making the right of access more effective, suffer from technical deficiencies.[932] Organisations must provide this access with robust mechanisms for user authentication and through secure channels to prevent leakage.[933] Such repositories have to be designed accordingly right from the start, as later adaptation will often be expensive and difficult.[934] A similar conflict between the right of access and data security can be observed in relation to Privacy by Design (PbD) technologies, whose aim is to limit access to data – exactly the opposite of what a data subject is seeking.

6.5.2. Enablers to data subjects' control

As explained above, the right of access proves important because of the values it safeguards; privacy, self-determination, and democracy are only the most important ones. Tene and Polonetsky contend that to leave this opportunity untapped would be value minimising.[935] Access requests filed in the aftermath of the recent Facebook and Cambridge Analytica scandal confirm the indispensability of the right in the modern era. Professor Carroll, a US citizen, used his right of access to request that Cambridge Analytica, a data mining company that allegedly harvested and manipulated information about millions of voters, hand over his personal data to help him understand how his voting behaviour was influenced.[936] Caroll's fear was that the manipulative use of personal data in the pre-election

---

928 Tene and Polonetsky (2013) 255.
929 Ibid.
930 Deborah Lupton, 'Personal Data Practices in the Age of Lively Data' in Jessie Daniels, Karen Gregory and Tressie McMIllan Cottom (eds), *Digital Sociologies* (2015) 10.
931 Tene and Polonetsky (2013) 268.
932 See for example 'MyHeritage Statement About Cybersecurity Incident' (*MyHeritage Blog*, 4 June 2018) <https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/> accessed 5 August 2018.
933 Tene and Polonetsky (2013) 243.
934 Ibid.
935 Tene and Polonetsky (2013) 268.
936 Donie O'Sullivan, 'New York professor sues Cambridge Analytica to find out what it knows about him' *CNN* (18 March 2018) <https://www.cnn.com/2018/03/17/politics/professor-lawsuit-cambridge-analytica/index.html>accessed 8 June 2018.

period undermined his autonomy to exercise his voting rights and participate in the democratic choice in an un-biased way.

Carroll's request for access was granted but the data he received did not fully disclose how the firm arrived at its predictions on voting behaviour. Hoping that he will finally be able to access the full set of data that the company holds on him and determine what impact it had on his voting behaviour during the elections, Carroll is now suing the company at a British court of justice.[937] The GDPR's updated provision in Article 15 could give data subjects who are bringing claims similar to Carroll's more leeway to access data on algorithmic decisions.[938] Besides individuals, some other actors, (e.g., non-governmental organisations) are using the right to access to gain (useful) information.[939] Such collective use of data protection rights has the potential to heal problems related to data protection as an individual right, in particular those related to individual agency.

Another enabler to the right of access in the GDPR is a financial one. Article 15 includes the requirement that the first copy of data be free of charge. This gives an incentive to individuals to more often request their information. In the same vein, the requirement that access should in principle be available electronically lowers costs and saves time for data subjects making requests.

Apart from the novelties regarding the law in books, some practical solutions seem to foster the right of access even more. As explained above, if the right is tied to a commercial service, it is more likely to be exercised. Moreover, if the right is implemented in a way that is user-friendly (e.g. offering a simple and open interface), more individuals may decide to exercise it.[940] Finally, the right of access might be fostered by developments in the area of blockchain technology[941] and AI.

6.6. Conclusions

Chapter 6 sought to answer the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection laws, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* This research sub-question is considerably broad as it refers to data subject rights as a whole. Chapter at hand, however, narrowed it down to the right of access.

Section 6.2. to 6.5. explored what the right of access entails and in what ways it contributes to data subject control. Section 6.2. introduced the provisions of Article 15 and illustrated how the application of the right is affected by the forces of the data-driven economy. Further limitations were revealed using a short analysis of some practical application of the right in section 6.4. Indeed, many barriers to the right stem from the new realities in the data-driven economy, in particular the outspread reuse of data and combinations, and the specific nature of modern information platforms. However, there are

[937] Ibid.
[938] See for example Lilian Edwards and Michael Veale (2017) 24.
[939] See current projects by nyob, a professional privacy enforcement NGO founded by Max Schrems <https://noyb.eu/projects-2/> accessed 27 December 2018.
[940] However, the danger that such (typically commercial) implementation may be too restrictive remains present.
[941] Before blockchain is actually used as a medium to make requests, it is of utmost importance that possible negative consequences for individual privacy are carefully assessed before blockchain becomes operable. One such solution could be the use of a private blockchain.

numerous undeniable benefits of someone's access to and scrutiny of data. In the future, new technologies and/or the extended GDPR scope may help make the right more effective.

7. THE RIGHT TO BE FORGOTTEN

7.1. Introduction

It is part of human nature that we are prone to forgetting our ideas and achievements. Luckily, the same goes for our failures. In fact, forgetting is the default setting of the world we know and with which we feel comfortable. Knowing that time is an unbeatable opponent quiets us down and offers us a sense of restored self-dignity.

In the 21st century, in the age of big data, the default of forgetting has changed fundamentally. As was shown in Chapter 2, the amount of information that current technology is able to process and store allows for storage of basically every single piece of information out there. In August 2017, IBM scientists managed to fit a record 330TB[942] of uncompressed data into a small cartridge.[943] Due to the limitless availability of storage and highly effective techniques to search for interesting information in the mass of data, there is no more need to decide what to preserve.[944] Everything is remembered, recorded in the spaces (in the cloud) of a web which by itself does not have any procedure to forget.[945]

Moreover, the limitless use of data presents a relatively cheap and unexploited business opportunity, which can considerably easily translate into profit. Thus, the demand for personal data collection and processing is increasing. However, this development comes at a cost: little consumer knowledge of and control over what information is being processed for corporate gain.[946]

As technology and markets have created a situation (default remembering) that diametrically contrasts the one that we consider normal (default forgetting),[947] it is not surprising that regulators have pushed forward some legal measures to mitigate the imbalance. In the EU, the right to be forgotten (RTBF) is one such measure, but more legislative initiatives have started all around the world.[948] The idea that underpins all these mechanisms is the fear of losing control over personal data, which comes as a necessary consequence of information overload, power imbalances, and informational insecurity.

Chapter 7 seeks to answer the fourth research sub-question regarding the entitlements that data subjects enjoy under the data protection laws, the implications of the data-driven economy for these rights and the extent to which these entitlements afford control to data subjects. As this sub-question is considerably broad, it is addressed in several chapters. In this chapter, it is narrowed down to the right to be forgotten, exploring the scope and control-enhancing potential of the right. Although the

---

[942] TB (tera byte) is a unit of information equal to one million (10^{12}) or strictly, 2^{40} bytes. This equals 1000 GB or, which is the same capacity as eight of the biggest iPhones. 1 TB storage suffices for saving a ton of information – e.g. 80 HD movies.
[943] Bradly Shankar, 'IBM scientists have fit a record 330TB of uncompressed data into a small cartridge' (3 August 2017) <https://mobilesyrup.com/2017/08/03/ibm-scientists-330tb-uncompressed-data-tape-cartridge/> accessed on 9 June 2018.
[944] Elena Esposito, 'Algorithmic Memory and the Right to Be Forgotten on the Web' (2017) 4 Big Data & Society.
[945] Ibid.
[946] Illegally held personal data by the company Cambridge Analytica was used for inappropriate uses such as voters' manipulation. The company promised to delete the illegally obtained databases but the recent reporting shows that the opposite was true. Nick Statt, 'Cambridge Analytica reportedly still hasn't deleted Facebook user data as promised' *The Verge* (29 March 2018) <https://www.theverge.com/2018/3/29/17176866/facebook-cambridge-analytica-data-still-not-deleted-colorado-users> accessed 8 June 2018.
[947] Mayer-Schönberger and Cukier (2014) 15.
[948] See a good overview in: Gregory Voss and Celine Castets-Renard, 'Proposal for an International Taxonomy on the Various Forms of the "Right To Be Forgotten": A Study on the Convergence of Norms' (2016) 14 Colorado Technology Law Journal 281.

focus is on the RTBF as defined in the GDPR, the RTBF is also understood in a broader sense, i.e. including all the legal entitlements that facilitate 'forgetting', either perpetual or temporary, as well as non-legal mechanisms such as obfuscation.[949]

To answer that question, this chapter proceeds as follows. First, section 7.2. explains the values protected by the RTBF and why they are under pressure. Then, section 7.3. provides a brief summary of the roots of the RTBF, and section 7.4, reviews relevant case law. Section 7.5. subsequently describes different types of legal entitlements that aim to facilitate forgetting to afford individuals active control over data. Several entitlements are distinguished: the right to erasure or 'the right to be forgotten in the narrow sense' (Article 17 of the GDPR), the right to object (Article 21 of the GDPR), and some other legal and technical manifestations. In particular, the right to erasure in Article 17 is analysed in detail through the lens of the data-driven economy. The final section assesses the value of the RTBF in the context of the data-driven economy and provides the background information for Chapter 10, where solutions to its shortcomings are explored in more detail.

7.2. Values underpinning the RTBF

The RTBF interacts with several fundamental values that focus on the protection and flourishing of someone's personality. These are privacy, data protection, autonomy, and human dignity.

As an instrument of control,[950] the RTBF corresponds to the active side of privacy, often labelled 'privacy as control', and in particular to the right to data protection.[951] 'Privacy as control' suggests that an individual has the power to principally determine the dissemination and use of information concerning his person.[952] In the context of the data-driven economy, this control can be easily undermined once material is published online, since what follows is most often perpetual reminding and remembering.[953] One example is the activity of search engines, which may store or link to past versions of webpages through caching.[954]

Chapters 5 and 6 established that both the right to information and the right of access are manifestations of the 'personal data control' idea. Another typical instrument of this idea is consent, as it gives an individual the power to say yes or no to data processing. Notably, the RTBF offers the option to reconsider and change a decision on personal data processing, even in cases where the processing started without the data subject's consent. Furthermore, the right also provides data subjects with the possibility to influence data processing that has taken place outside the (first) data

[949] Discussed below in section 7.5.2.4.
[950] In De Hert and Gutwirth's words, control is linked to 'privacy as transparency' (as opposed to 'privacy as opacity'). De Hert and Gutwirth (2006) 69-70. Lynskey associates control with the fundamental right to data protection. Lynskey (2015) 11.
[951] For a discussion on the subtle difference between data protection and privacy see Chapter 3, section 3.2.2.2.
[952] Lilian Mitrou and Maria Karyda, 'EU's Data Protection Reform and the Right to Be Forgotten - A Legal Response to a Technological Challenge?' (2012) 10 <http://www.icsd.aegean.gr/website_files/proptyxiako/388450775.pdf> accessed 8 June 2018.
[953] Ibid. See also Mayer-Schönberger and Cukier (2014) 176.
[954] Voss and Castets-Renard (2016) 290-291.

controller's premises.[955] For these reasons, the RTBF can be described as one of the strongest manifestations of control in EU data protection law.

The objectives of the RTBF can be further related to the idea of informational self-determination, as a reflection of a person's autonomy in the digital age.[956] After all, the RTBF conveys the idea of empowering individuals against data processing entities – even the most powerful ones, such as search engines – by guaranteeing the '*authority of the individual in principle to decide for himself whether or not his personal data should be divulged or processed*.'[957] This is at the heart of the notion of informational self-determination. Taking one step forward, the RTBF can be linked to human dignity. The RTBF limits dissemination of personal data to enhance consumer protection against widely spread commercial exploitation, which often treats people as mere objects rather than subjects.[958]

7.3. Towards the GDPR's version of the RTBF

This section introduces two rights that preceded the GDPR's version of the right to be forgotten: the right to oblivion that emerged in the criminal law, and the right to erasure (including some related entitlements) in the DPD.

7.3.1. The right to oblivion in criminal law

The RTBF is a manifestation of the right to oblivion in the digital age. Originally, the right to oblivion was introduced to be invoked in cases where undesired public exposure was given to a person's past.[959] It was meant to work as a shield against disproportionate intrusion by mainstream media (papers, news broadcasts, radio shows, etc.) into the private life of people who had entered into the public eye.[960] A special form of the right to oblivion had been developed in criminal law. This right ensured that someone could preclude others from identifying him in relation to his criminal past.[961] The right focused not so much on the deletion of data, but on regulating (blocking) the (re)use of data.[962] Thus, the underlying idea was to prevent secondary users of the data, apart from a judicial body, from using the fact to the individual's disadvantage. As is shown below, the RTBF in the big data context functions similarly. The key goal is to limit negative effects of data *re*use. Recital 66 of the GDPR acknowledges that the mission of the right is to empower and protect individuals against modern online data processing, which implies a focus on secondary rather than primary uses of data.

---

[955] See below Section 7.4.2.1.2. However, under Article 13 of the EU e-commerce directive, companies must regularly check their caches to detect any changes to the original source to avoid liability. This rule to some extent limits the storage of online information but as long as the original website remains unchanged, the copy in the cache is kept.
[956] Giancarlo F Frosio, 'Right to Be Forgotten: Much Ado about Nothing' (2017) 15 Colorado Colorado Technology Law Journal 307, 313-314.
[957] Ibid.
[958] Tsesis (2014) 141.
[959] Hans Graux, Jeff Ausloos and Valcke Peggy, 'The Right to Be Forgotten in the Internet Era' in J Pérez, E Badía and R Sáinz Peña (eds), *The Debate on Privacy and Security over the Network: Regulation and Markets* (Ariel 2012) 96.
[960] Ibid.
[961] Franz Werro, 'The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash' in Aurelia Colombi Ciacchi and others (eds), *Haftungsbereich im dritten Millennium / Liability in the Third Millennium* (Nomos 2009) 285, 291.; see for example the Slovenian Criminal Code (Kazenski zakonik), Chapter 9, article 193 – Legal rehabilitation and deletion of the verdict (Zakonska rehabilitacija in izbris obsodbe).
[962] See for instance (2011) 5.

7.3.2. The RTBF under the data protection directive

The policy and scholarly discussion on the RTBF erupted some time before the GDPR was adopted. Although the data protection directive (DPD) did not mention the RTBF explicitly, it was indeed present implicitly.[963] This was later unanimously confirmed by the CJEU in Google Spain.[964] In fact, the Court noted that the DPD contained more than one single legal basis for 'online forgetting'. Indeed, looking at the DPD text, it is possible to distinguish three bases: the right to erasure (Article 12 of the DPD), the right to object (Article 14 of the DPD), and the withdrawal of consent.[965]

7.4. The RTBF under the GDPR

7.4.1. The CJEU paving the way towards the GDPR in line with the 2012 proposal

In 2012, after it emerged with the proposal for the data protection law reform, the European Commission (EC) declared the RTBF an independent right and the first pillar of informational control.[966] Specifically, this early version of the GDPR stated that the main purpose of RTBF was to protect children from the negative effects of their reckless behavior on social networks.[967] The RTBF was one of the most attention-grabbing parts of the EC's proposal, although it fell short of being a new legal concept.[968] As mentioned above, the DPD already included the principles underpinning the RTBF.[969] Save for some new duties for data controllers[970] and a clearer articulation of the right, what the proposal for the GDPR brought was more of a symbolic gesture than a material change.[971] Nevertheless, the declaratory power should not be disregarded.

During the GDPR negotiations, the CJEU took some pioneering steps towards reawakening data subject rights. Its creative approach was in line with the emphasised role of the RTBF in the EC 2012 proposal. The following section analyses two key CJEU decisions. In both decisions, the Court used the RTBF to tackle the problem of control in the online environment. The decisions were adopted before the GDPR entered into force and thus they applied the provisions of the 1995 DPD. By adopting a lenient

---

[963] Ibid.

[964] C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 (Google Spain).

[965] For a detailed analysis of the DPD see Jef Ausloos, 'The "Right to Be Forgotten" - Worth Remembering?' (2012) 28 Computer Law and Security Review 143.

[966] Viviane Reding, 'Your data, your rights: Safeguarding your privacy in a connected world; speech for Privacy Platform "The Review of the EU Data Protection Framework" in Brussels, 16 March 2011' <http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm> accessed 7 June 2018.

[967] 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) 1 final, article 17.

[968] In *Google Spain* the Court of Justice of the European Union made it clear that the right to be forgotten is encompassed in the fundamental right to privacy. See also Christopher Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2015) <http://eprints.lse.ac.uk/61584/> accessed 8 June 2018.

[969] The right to be forgotten was reflected in the right to objection and deletion. European Commission, 'Factsheet on the "Right to Be Forgotten" ruling' <http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf> accessed 8 June 2018. Also, it is interesting to note that the legislator struggled with the name. The EC proposal from 2012 included the right to be forgotten. After the Parliament's amendments, the provision was reworded into the right to erase. In the latest version of the GDPR proposal, the right to be forgotten is explicitly mentioned as a synonym for the right to erasure in Article 17.

[970] The duty to make sure that third parties are informed about the request for erasure and in some, limited cases, the controller would be held responsible for making sure that third party processors comply with the erasure request (Article 17(2) of the 2012 GDPR's proposal).

[971] Voss and Castets-Renard (2016) 290; Tjong Tjin Tai (2017) 307.

interpretation of the DPD, the CJEU came close to the contemporary definition of the RTBF under the GDPR.

7.4.1.1. Google Spain

In 2014, the landmark *Google Spain* decision established the RTBF in relation to search engines, or, more precisely, the right to remove inaccurate, irrelevant, or otherwise incompatible links that contain personal data.[972] It is important to note, at the outset, that the interpretation of the RTBF is not the only emphasis of the judgement. Rather, the judgement makes a radical decision concerning the responsibilities and legal nature of search engines such as Google, Bing, Yahoo, etc. Establishing their responsibility as data controllers, however, directly impacts the duties in relation to data subject rights, including that of erasure (the RTBF in the narrow sense). This is why the judgement was labelled as a landmark decision on the RTBF and why it is significant for the analysis in this chapter.

The key highlights of the judgement are the following. First, the CJEU found that what Google engages with is personal data processing as defined in Article 2(b) of Directive 95/46. Specifically, the Court highlighted the activities of the search engine as '*exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine "collects" such data which it subsequently "retrieves", "records" and "organises" within the framework of its indexing programmes, "stores" on its servers and, as the case may be, "discloses" and "makes available" to its users in the form of lists of search results.'*[973] The list of results created as a follow-up to an individual query offers a structured overview of the information relating to that individual that can be found on the Internet, enabling Google to establish a more or less detailed profile of the data subject.[974] This is something different than having the information merely stated somewhere on the web. In fact, these activities may profoundly, even more than those of the publishers of the websites, affect the fundamental right to privacy. In the holding, the Court stressed that since search engines played a decisive role in the overall dissemination of this data, they should be regarded as controllers, *i.e.* entities determining the purposes and means of the processing activity.

By establishing that Google is a data controller, the Court made it possible to hold the company responsible for protecting personal data.[975] This responsibility includes ensuring that data subject rights, such as the right to erasure and the right to object, are respected.[976]

In the judgement, the Court applied two DPD rights: the right to erasure and the right to object. The former (Article 12(b) of the DPD) provided that *particularly* when data appeared to be incomplete and inaccurate, the data subject should have the right to request erasure. The latter (Article 14 (a)) allowed for objection on the basis of a data subject's compelling legitimate grounds. The Court made it clear, however, that erasure and objection were possible in all cases when personal data was processed in a way non-compliant with the principles of data protection as listed in Article 6 of the DPD. In other

---

[972] *Google Spain*, para. 88.
[973] *Google Spain*, para. 28.
[974] *Google Spain*, para. 80.
[975] Under Article 4 of the GDPR (Article 2 of the DPD) controllers are those who determine what happens with personal data and therefore bear responsibilities to protect data including that to delete data. See more on the notion of controller in Chapter 3, section 3.3.2.1.2.
[976] The Court then went on establishing the territorial scope of the directive and found that Google's activities, through its office in Spain, fell within the scope (see *Google Spain*, para. 21-41).

words, erasure could be triggered when data was inadequate, irrelevant or no longer relevant, or excessive in relation to initial purposes and in light of the time that had elapsed.[977] In particular, the court pointed to the principle of lawful data processing.[978] This principle was detailed in Article 7, listing several bases for legitimate processing of data.[979] Paragraph (f) of the latter article was of particular importance for Google, as it stipulated that data could be processed if this was necessary for the legitimate interests of the controller or third parties.[980] The court stressed that the basis in Article 7(f) could not be generally used by data controllers. Instead, a careful weighing of the interests had to be carried out: fundamental rights of data subjects on the one hand, and interests of the controller and third parties to whom the data was revealed on the other.[981] If the balancing test showed an imbalance, this gave rise to the RTBF and to the right to object.[982] To establish a data subject's interest, it was not necessary to show that non-removal of the data would cause any prejudice against her.[983] In the final part of the holding, the Court considered the right to data protection of data subjects in light of possible interference with commercial interests of search engines and freedom of information of Internet users. Contrary to the AG opinion, the Court found that Google's economic interest and the public's interest in personal data (specifically, the links to the applicant's auction notices) could not outweigh data subjects' fundamental rights.[984] As a result of this interpretation, it was found that the applicant, Mr Costeja, had the right to ask for erasure.

Besides the right to erasure, the Court indicated that the right to object could also be used as a legal basis for 'forgetting' (Article 14(a)). Under the DPD, the right to object to the data processing could be invoked when the subject put forward compelling and legitimate grounds. The right to erasure and the right to object to the data processing actually overlapped significantly.[985] Indeed, when a data subject had compelling grounds to object to an otherwise lawful processing, the conclusion could be reached that 'the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed' were in fact 'overridden by the interests for fundamental rights and freedoms of the data subject,' and thus that the data controller lacked legitimate grounds for the processing under Article 7(f) of the DPD.[986] In turn, lack of such grounds would make the processing non-compliant with the DPD provisions, allowing the data subject to exercise the right to erasure under Article 12(b).[987] In section 7.4.2.2.1., it is explained how the GDPR resolved the overlap.

---

[977] *Google Spain*, para. 70.
[978] *Google Spain*, para. 95.
[979] See also Section 3.3.2.1.2.1.
[980] Purpose specification principle states that data the purpose of collection must be determined at the time of collection of the data and that later the data cannot be processed in a way incompatible with those purposes. See also Fanny Coudert, Jos Dumortier and Frank Verbruggen, 'Applying the Purpose Specification Principle in the Age of "big Data": The Example of Integrated Video Surveillance Platforms in France' (2012) <https://www.law.kuleuven.be/icri/>.
[981] *Google Spain*, para. 74.
[982] *Google Spain*, para. 75-76.
[983] Ibid.
[984] <https://epic.org/privacy/right-to-be-forgotten/> accessed 8 June 2018.
[985] Interestingly, the Slovenian data protection act (*Zakon o varstvu osebnih podatkov* from 2004, Article 32) conveniently places the two rights in the same article and apply the same set of procedural rules regardless of the right that is eventually invoked. The Italian data protection act follows this pattern as well (*Codice in materia di protezione dei dati personali* from 2003, Article 7(3)). The GDPR took a different approach and separated the provisions in two articles.
[986] Peguera (2016) 546.
[987] Provided that the consent of the individual is absent. Ibid. A balancing is also needed under Article 14(a) to determine whether the data subject may *object* on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. According to the CJEU, that balancing

The Court's understanding of the RTBF clearly corresponds to the DPD provisions in Articles 12 and 14,[988] but some commentators have pointed out that what the Court did was not an application of the right to object and erasure *per se.*[989] Rather, the court created a right to de-index or delist search results. In this regard, it should be noted that *'[the court] did not rule that search engines can be compelled to interfere with the source itself, nor that search engines can be compelled to delist a search result entirely (i.e., on the basis of any search term).'*[990]

In my view, delisting should be seen as a subcategory of deletion of personal data as it is meant to protect, to a large extent, the same values.[991] Personal data is the information about an individual that is available on the source website, but equally so the collection of URLs that appear as a search result when a name is used as a search term. In a sense, delisting of search results is erasure of reused data. Of course, delisting should not evolve into the one stop shop right to delist of any link made when your name is entered into Google. Vanishing yourself generically from web-search could have serious implications for the right to freedom of expression (Article 11 of the EU Charter).

As delisting of search results is erasure of reused data, it comes naturally that it cannot be done in the same way as in the case of primary data erasure. However, erasure is still possible to some extent. In fact, erasure of some search results may better protect individuals in the data-driven economy than actual deletion of the sources (supposing that a query still yields results even though the source has been deleted),[992] because it prevents the creation of intrusive or misleading profiles and their unlimited disclosure.[993]

The Google Spain judgement received massive media attention and some academic criticism too, in particular due to the Court's strong preference for privacy over freedom of speech, expressed in the (allegedly too vague and brief) proportionality test conducted in the judgement.[994] The balancing of the right to privacy/data protection and the freedom of expression was particularly provoking. In fact, the RTBF as created by the CJEU was condemned as the greatest threat to free speech and as censorship of the Internet.[995] In the meanwhile, national DPAs and courts seem to have been able to strike a balance. In fact, when weighing the right to data protection against freedom of speech, the courts have been protective of the latter.[996] Even Mr Costeja, the applicant in the Google Spain case,

---

'*enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation.*' *Google Spain*, para 76.

[988] The Court is consistent: 'Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that […] the operator of a search engine is obliged to remove from the list of results [...].' *Google Spain*, para 88.

[989] See for instance Aleksandra Kuczerawy and Jef Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Colorado Technology Law Journal 219, 224.

[990] Ibid.

[991] With *objectives* it is meant *values*; see above the section on values.

[992] Deleted websites may still appear on Google, may be saved in cache and sometimes even an indication of the fact that the website has been deleted is telling. Mitchell Wright, 'Why Is Google Still Indexing My Deleted Pages?' (*SEOblog*,4 June 2014) <https://www.seoblog.com/2014/06/google-indexing-deleted-pages/> accessed on 15 June 2018.

[993] *Google Spain*, para. 87.

[994] *Google Spain*, para. 87.

[995] Jeffrey Rosen, 'The Right to Be Forgotten' [2012] Stanford Law Review Online 88 <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/> accessed 8 June 2018.

[996] Stefan Kulk and Frederik Johannes Zuiderveen Borgesius, 'Freedom of Expression and "Right to Be Forgotten" Cases in the Netherlands After Google Spain' (2015) European Data Protection Law Review 113.

was eventually denied his right to erasure.[997] On similar grounds, a court in the Netherlands rejected an applicant's request for his criminal past to be removed.[998]

Julia Powles' commentary puts the discussion about Google Spain and freedom of speech in a different light. This is how she starts her reasoning: '*if we concede that the internet is public space, that the web is the public record, then Google, on its logic, is the custodian and indexer of our personal records.*'[999] This is in essence Google's argument for a weaker RTBF and a stronger freedom of speech. However, Powles argues that a handful of Internet services is not the same as the real public record guaranteed by law, from archives, and even from human memory itself. These are the true information custodians, which will all continue to be available when Google ends.[1000] Thus, claiming that the RTBF should not apply to Google because of its role in enabling freedom of information and speech seems to be inappropriate.

Considering the judgement in *Google Spain* from a distance, it is right to argue that it had a far-reaching impact. Immediately after the CJEU judgement in 2014, Google started receiving numerous requests for the RTBF. Out of approximately 966,377 requests received by Google so far (8 June 2018), deletion was granted to approximately 43%.[1001] However, there are some negative aspects of the RTBF system as it was built by Google. First, it is disputable whether Google, as a private entity, should be granted the responsibility to adjudicate between someone's privacy interests and the interest of the general public in information.[1002] Second, Google's internal RTBF procedure lacks transparency. Apart from the general numerical reports on the outcomes, Google's decision-making process remains silent and opaque, with little public process or understanding of delisting.[1003] Third, erasure from the search engine's index has no impact on original sources, which remain available to anyone interested. While it is true that those sources are likely to be found only though search engines, they may still violate privacy in cases when the searcher knows for which webpage to look. Finally, to date, delisting is only effective on European servers, since Google rejected EU demands for a worldwide application of the RTBF. This means that the data that has been deleted in the EU may still be accessible via the US server.[1004]

Through the lens of data subject control, however, the Google Spain decision was a step forward. In this case, the RTBF proves important because it adds exactly what was missing in the idea of control under data protection law. First, it allows for *control over secondary data reuse and data flows.* The

---

[997] Frosio (2017) 13.
[998] Kulk and Zuiderveen Borgesius (2015).
[999] Julia Powles and Enrique Chaparro, 'How Google determined our Right to be Forgotten' *The Guardian* (18 February 2015) <https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search> (accessed on August 11, 2017).
[1000] Ibid. Further, the authors warn that despite of its global nature and overall usefulness, Google remains a private party seeking primarily for its own profit and benefits, even though this may involve manipulation of its billions of users.
[1001] Some recent judicial cases show that the applicants attempt to take the right to be forgotten to its edges, transforming it into a facilitator of not only data protection and privacy but also other interests, such as preservation of commercial interests and the fight against defamatory comments or fake news. Helena Ursic, 'In The Anticipation Of The Right To Be Forgotten's 3rd Birthday – EU Courts In Search Of Boundaries, Coherence And Balance' (*Internet Interdisciplinary Institute*, 30 March 2017) <http://www.theiii.org/index.php/1981/in-the-anticipation-of-the-right-to-be-forgottens-3rd-birthday-eu-courts-in-search-of-boundaries-coherence-and-balance/> accessed 9 June 2018.
[1002] See for example Eldar Haber, 'Privatization of the Judiciary' (2016) 40 Seattle University Law Review 115.
[1003] Kuczerawy and Ausloos, 245.
[1004] The case is currently pending at the CJEU. CNIL's press release at <http://www.conseil-etat.fr/Actualites/Communiques/Droit-au-dereferencement> accessed 8 June 2018.

consent mechanisms and control rights are in principle effective as far as (simple) primary data use is concerned. This is actually what they were created for.[1005] Chapter 2 showed that the greatest risks of the data-driven economy come from data reuse. In relation to those risks, however, consent and data subject rights often appear ineffective.[1006] Still, the RTBF as applicable to Google is one of the rare cases where the risk of data reuse was directly addressed. Second, the case showed that *control needs strong technical and policy backing to be effective.* Following the judgement, Google created a system of online URL removal, which is effective (as it is workable), user-friendly, and considerably fast. This system gave individuals the motivation to apply the right and it reduced the administrative burden on the individual, although administration costs become high when an individual wants to challenge a decision due to the system's opaque internal logic.

7.4.1.2. Manni

In *Manni*, the CJEU had to determine whether an entrepreneur has the right to demand deletion of his personal data from a commercial register.[1007] In some sense, a register can be compared to Google's search engine: it comprises a number of entries and, by making them publicly available, facilitates their dissemination.

The dispute started when *Manni*, an Italian entrepreneur, sued the Lecce Chamber of Commerce for not removing his personal data from its commercial register.[1008] Manni contended that if his name in the register could be associated with a dissolved company, this would negatively impact his reputation and therefore infringe his privacy. A particular danger was posed by the fact that data from the register could be *reused* (and in fact had been *reused*) by rating agencies specialised in the collection and processing of market information and in risk assessment.

The CJEU denied Manni the RTBF (erasure). In the analysis, it balanced the right to privacy and data protection, and the right to publicity (i.e., the objectives of legal certainty and protection of third parties),and decided that the latter prevailed. Two arguments supported the judgement: 1) the commercial register only disclosed a limited number of personal data items, and 2) Manni deliberately chose to participate in trade and should have known that certain publicity was an indispensable part of it. However, the Court pointed out that in exceptional circumstances Manni might have the right to object, *i.e.* an alternative control right under DPD. 'This right enables that account is taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.'[1009] Unfortunately, the Court did not elaborate on when this right could apply.

Contrary to the Google Spain case, the Manni judgement was criticised for not assigning adequate weight to privacy risks. As Kulk and Borgesius note, in the digital age every online publication might have fatal effects on someone's privacy: *'If a public register is published online, its data can be collected*

[1005] See the historical analysis in Chapter 4, section 4.4.
[1006] See more detailed analysis in Chapter 10.
[1007] C 398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni* [2017] ECLI:EU:C:2017:197 (*Manni*).
[1008] Registering commercial entities and their directors is a legal obligation in Italy (as well as in some other EU countries). *Manni*, recital 19. The rationale behind the publicity is, among others, protection of (future) commercial transactions between companies and third parties.
[1009] *Manni*, recital 47.

and republished by data brokers, journalists, search engines, and others. Such data re-use can serve important goals […]. However, data re-use can also threaten privacy.'[1010] Zanfir, while supporting the CJEU ruling, also acknowledged the important point that Kulk and Borgesius made, noting that there is still room for improvement in *'analysing the proportionality of the interference of the virtually unlimited publishing* [underlined by H.U.V.] *of personal data in the Companies Register with Articles 7 and 8 of the Charter.'*[1011]

Another explanation for why the RTBF did not outweigh the publicity principle in *Manni* could be that his privacy expectations were not met due to the entrepreneurial nature of the index and the limited availability of data. If the trader could have used the right to remove the limited set of personal data which he agreed to submit in exchange for being allowed to join the commercial community, it would have been the privacy of his business that would gain protection but not (necessarily) him as a natural person. From the assertions of the applicant, no particular concern about the privacy of his person can be inferred. Rather, it seems that his commercial rather than personal reputation was at stake.

Nevertheless, in light of the growing importance of data-driven processing, Kulk and Borgesius' observation remains pertinent. Intrusions in someone's commercial reputation can have an impact on her personal life and lead to personal privacy intrusions. This is even more likely when data is available to third parties for reuse and exposed to potential repurposing. Although such data reuse's implicit privacy threats seemed to be insufficient to tilt the balance in the *Manni* case, they should not be disregarded. In fact, it would be helpful if the Court acknowledged the odds of ubiquitous data reuse more directly, as it did in Google Spain. After all, these odds might urge the need for the RTBF. At least, the impact of the data-driven economy could contribute to a data subject's particular situation and in turn give rise to the right of objection.[1012]

7.4.2. The RTBF and its manifestations under the GDPR

The previous section (7.4.1.) suggested that the provision on the right to erasure in the 2012 GDPR proposal was not revolutionary. Nonetheless, the GDPR introduced some new duties for data controllers[1013] and provided a clearer articulation of the right.

The remainder of this section provides a detailed analysis of the relevant provisions under the GDPR. Furthermore, the section considers two other legal entitlements under the GDPR, the right to object and the possibility to withdraw consent, that also facilitate digital 'forgetting'.

[1010] Stefan Kulk and Frederik Zuiderveen Borgesius, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018).

[1011] Gabriela Zanfir-Foruna, 'CJEU in Manni: data subjects do not have the right to obtain erasure from the Companies Register, but they do have the right to object' (*pdpEcho*, 13 March 2017) <https://pdpecho.com/2017/03/13/cjeu-in-manni-data-subjects-do-not-have-the-right-to-obtain-erasure-from-the-companies-register-but-they-do-have-the-right-to-object/> accessed 9 June 2018.

[1012] For example, personal data from the commercial register could be linked to data gathered by a data broker. If combined, the data set could lead to a detailed profile of a private citizen.

[1013] The duty to ensure that third parties are informed about the request for erasure. In some limited cases the controller would be held responsible for making sure that third party processors comply with the erasure request (Article 17(2) of the 2012 GDPR's proposal).

7.4.2.1. Analysis of Article 17 of the GDPR – the right to erasure or the (explicit) RTBF

7.4.2.1.1. General

Under the GDPR, data subjects have the right to obtain erasure of their personal data without undue delay (the RTBF in a narrow sense). The right can be asserted on multiple grounds.

Article 17(1)(a) of the GDPR explicitly allows data subjects to seek the deletion of data that is no longer necessary in relation to the purposes for which it was collected or otherwise processed. This diction emphasises the importance of the principle of limited and specified purpose of personal data processing. The restatement of the principle of purpose limitation is a positive improvement, because data is increasingly used for secondary purposes.[1014] The right to erasure seeks to prevent those uses that fall short of being relevant for the primary data purpose (and which, most likely, do not meet users' privacy expectations). However, it will often be difficult to establish that the data should be forgotten on the ground of 'no longer being necessary for the purpose for which it was initially collected'.[1015] In an increasingly personalised Internet, almost every bit of personal data can be argued to be relevant.[1016] Moreover, to allow unforeseen future uses, data processing is often based on vague purpose definitions. This means that any secondary use can be interpreted as relevant in relation to the purposes for which the data was collected.[1017] Such an approach fundamentally challenges not only the idea of purpose limitation but also the effectiveness of the RTBF.[1018] Even so, from the perspective of a data subject, 'being relevant for the initially set purposes' may be interpreted differently than from the perspective of a data controller. The Court in *Google Spain* stated: 'All the circumstances should be taken into account'.[1019] This indicates that both viewpoints should be considered in the final decision. In other words, the decision should balance the interests of all parties involved with due regard to their fundamental rights.

Article 17(1)(b) of the GDPR foresees erasure if consent is withdrawn and there is no other legal basis for the processing.[1020] The withdrawal of consent only stops data processing *ex nunc*.[1021] By applying the right to erasure, however, a data subject has the option to also achieve an *ex tunc* erasure.[1022] Besides the withdrawal of consent and non-compliance with the purpose specification principle, the GDPR provides a few other grounds for the right to erasure. Erasure may be required by a provision in a national law or can be requested if processing is unlawful, i.e. conflicts with legal rules in the GDPR and/or beyond it (Article 17(1)(d)). Erasure may also follow a successful objection request (Article 17(1)(c)). Finally, erasure may be triggered in a situation when personal data of children was collected

---

[1014] For example, a GPS device provider collects users' data so that it can offer a more personalised service. This is primary data use. The company then shares data with the government to help it analyse citizens' driving patterns and improve the road infrastructure accordingly. This is secondary data use. Such transfer is only allowed if users' have previously consented to it or if the company has a legitimate interest to share data, or in some other limited situations.

[1015] Bart Custers Bart and Helena Ursic, 'Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) 6 International Data Privacy Law 10.

[1016] Graux, Ausloos and Valcke (2012) 103.

[1017] Koops (2011) 244.

[1018] Ibid.

[1019] ' *… because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.' Google Spain*, para 94.

[1020] To achieve erasure on other grounds, a data subject will have to use 'the right to objection' route.

[1021] See section 7.4.2.2.2.

[1022] Ibid.

in relation to the offering of information society services, typically via social networks (Article 17(1)(f)). The regulator assumed that a person may want to remove personal data, especially on the Internet, if, when she was a child, she was not fully aware of the risks involved.[1023] The possibility that an adult seeks the removal of her childhood data is only foreseen in a recital, which makes it likely applicable but in no case binding (Recital 65).

Article 17's explicit declaration of the situations that amount to erasure does not mean any substantial change for individual control over personal data.[1024] As confirmed by the CJEU, the DPD already allowed erasure on more or less the same grounds, although in rather general terms. Under the DPD, data subjects could invoke this right whenever processing conflicted with the legal rules set out in the DPD, in particular because of incomplete or inaccurate data. While incompleteness and inaccuracy of data were a sign that erasure would probably be granted, any other conflict with a legal rule could in principle justify an erasure request.[1025] With regard to the erasure of a child's data collected via social media and other information society services on the basis of children's or parental consent, it should be noted that it only bears declaratory value. A withdrawal of either type of consent would justify erasure even if there was no specific provision to erase data under Article 17(1)(f).[1026] The special provision for such data would only be needed if some other legal basis for data processing was used.

Nevertheless, the reference to children's data is of special importance because it provides another perspective of the motivation for the right to erasure. In fact, the GDPR recitals suggest that forgetting the data generated by children is exemplary for the RTBF.[1027] At an early age, children are in a time of experimentation during which they test their boundaries, which is why it is critical that they be provided with a means of reinventing themselves as they mature and enter adulthood.[1028] Consider this case: at 14, a girl had posted some thoughtless comments on a blog about people from other countries. She is now trying to volunteer to work for a charity, but is terribly worried that they might see these comments of which she is now ashamed.[1029] The right to erasure could protect her from unacceptable and unforeseen risks by allowing her to remove the comment. In addition to children's own actions, adults may contribute to privacy and identity risks by oversharing personal materials such as new-born photos.[1030] Negative impacts of online sharing may worsen as a result of global distribution of the posts on social media and because screen-shots can lead to perpetual remembering. When such intrusions happen, children are often unable to object or act in any other way until they grow up. Thus,

[1023] The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child (Recital 65).
[1024] In a similar vein see Koops (2011) 244.
[1025] Provisions of Dutch and Belgian laws already had an extended the scope, also mentioning the purpose limitation. Korff (2002) 100.
[1026] As consent it is meant both a child's and parental consent. Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information & Communications Technology Law 146.
[1027] Recital 65 of the GDPR.
[1028] Draft OPC Position on Online Reputation <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/> accessed 9 June 2018.
[1029] Coleman Stephen and others, 'The Internet on Our Terms: How Children and Young People Deliberated About Their Digital Rights' (2017) 26 <https://casma.wp.horizon.ac.uk/wp-content/uploads/2016/08/Internet-On-Our-Own-Terms.pdf>.
[1030] Ramona Pringle, 'Today's kids will need right to remove online posts about them' *CBC* (31 January 2018) <http://www.cbc.ca/news/technology/pringle-kids-social-media-1.4510168> accessed 8 June 2018.

the RTBF that can be applied later in time helps children protect their privacy against intrusive data processing triggered by not only their own action but by their parents' actions as well.

The array of options with which an individual can ask for erasure of personal data is thus very broad. However, they are all subject to exceptions. The exception that protects freedom of speech and access to information (Article 17(3)(a)) is highly challenging. Personal data co-creates the Internet, the world's largest news and knowledge platform, and any removal clearly interferes with the rights to free speech and information. As already mentioned, the application of the RTBF in the *Google Spain* case was criticised for not paying sufficient attention to freedom of speech. When it comes to the GDPR, the opposite is true. The GDPR clearly acknowledges the exception of freedom of expression, and the same follows from the guidelines of the Article 29 Working Party.[1031] This indicates that the EU regulators are not stubborn when it comes to balancing privacy and freedom of expression, and that the impact of erasure on individual rights to freedom of expression and access to information will be limited.[1032]

Besides the right to information and freedom of expression, the right to erasure can be blocked by a rule in a national law, by an overriding public interest, or because of scientific, archiving, and other research reasons. Except for social networks and news platforms, data-driven companies do not typically facilitate the right of the public to information. Rather, they have economic and research goals. In some cases, the latter could lead to denial of the right to erasure. For instance, a hospital's AI processes large numbers of pseudonymised photos to help doctors pick the best treatment. Although the database is large, one photo might prove an indispensable source of information.[1033] Thus, due to scientific or health-care related reasons, the deletion request could be denied. However, it is difficult to foresee in what way the courts will interpret this GDPR exception – they may adopt a more restrictive approach.[1034]

Finally, it should be kept in mind that the right to erasure is limited due to the narrow material scope of data protection law. Only personal data can be erased, i.e. removed to the extent that its use is no longer possible.[1035] Aggregated and anonymised data sets are unaffected regardless of what harm the processing of such data may cause and how desirable its removal may be.[1036]

7.4.2.1.2. The meaning of 'informing third parties'

Compared to the *Google Spain* judgement, the GDPR's version of the RTBF is strengthened in one important aspect. Namely, it includes an obligation of the data controller that has made the personal data public to inform other controllers processing such personal data to erase any links to, or copies or

---

[1031] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' 11.
[1032] Frosio (2017) 9.
[1033] Roger Allan Ford and Nicholson Price, 'Privacy and Accountability in Black-Box Medicine' (2016) 23 Michigan Telecommunications and Technology Law Review 1, 34.
[1034] As some EU data protection authorities already did in the past. See for example the decision of the Slovenian DPA on the possibility to use health data on a large scope by medicine students. This was only possible based on patients' explicit consent or on a specific provision in law <https://www.ip-rs.si/vop/zdravstveni-podatki-pacientov-3058/> accessed 9 June 2018.
[1035] See for example the note from the Presidency of the Council of the EU to the Article 29 Working Party (note 3, page 2) <http://lobbyplag.eu/governments/assets/pdf/CD-6814_13.pdf> accessed 9 June 2018.
[1036] Bonnie Kaplan, 'Selling Health Data: De-Identification, Privacy, and Speech' (2015) 24 Cambridge quarterly of healthcare ethics 256, 261.

replications of, that personal data.[1037] In doing so, that controller should take reasonable steps, taking into account available technology and the means available to it, including technical measures.[1038]

Article 17(2) of the GDPR does not contain an obligation to erase or stop processing of data that has been made public (e.g., published on a website), but only an obligation to *'take all reasonable steps […] to inform third parties which are processing such data'* of the erasure request. The European Data Protection Supervisor has stated that Article 17(2) thus contains an obligation of endeavour instead of an obligation of result, and considers this '*more realistic from a practical point of view*'.[1039] Reading the provision carefully, however, this conclusion does not seem to be correct. In fact, the provision is an obligation of result: not with regard to the deletion of data, but with regard to the informing of third parties that have also published the personal data.[1040]

During the GDPR negotiations, several delegations expressed concerns regarding the enforceability of this rule.[1041] The data controller may not even be aware of all existing copies or replications of the data or of all the places where personal data has been disseminated.[1042] Solove and Schwartz warn that *'[t]his version of the RTBF raises complex questions regarding the precise obligations of the controller and downstream third parties, such as search engines and advertising networks, which have many innovative ways of collecting, tracking, and, in some cases, re-identifying data*.' To use an example other than a search engine, consider a data broker. Acxiom gathers data records from different sources and sells them to third parties. Consumers can contact Acxiom and request to have the information deleted, and Acxiom is then also obliged to inform all the thousands of parties with whom the data has been shared. However, there is no assurance that all of the personal data and third parties will be identified,[1043] let alone that the third parties will in fact remove the data.

To fulfil the obligation in Article 17 (2), data controllers may need to consider technical solutions to allow the tracking of bounces.[1044] For instance, major Internet services tend to create a link to the content and keep track of the link.[1045] Bartolini and Syri propose two opposite models for sharing content: a distributed model and a centralised model. In the former, data controllers keep track of all links that reference a given content (even if the data is replicated).[1046] In the latter, a given content exists in a single instance, and every dissemination of the data is simply a reference to the original data;

[1037] Hence, not only those to whom the personal data has been disclosed (this notification duty is different and stipulated in Article 19 of the GDPR).
[1038] Burri and Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479, 490.
[1039] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Data Protection Reform Package' (2012) 22 <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf>.
[1040] Joris van Hoboken, 'The Proposed Right to Be Forgotten Seen from the Perspective of Our Right to Remember (Prepared for the European Commission)' (2013) 15 <http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo Be Forgotten_Manuscript_2013.pdf> accessed 9 June 2018.
[1041] DE, DK, ES, FR, IE, IT, LT, LU, NL, PL, SE and UK. Materials from the GDPR negotiations in the Council (fn. 325) <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.
[1042] Kosta (2013) 253.
[1043] Sara Benolken, 'Digital ghosts: Deleted online footprints persist' (Willis Towers Watson Wire, 9 March 2017) http://blog.willis.com/2017/03/digital-ghosts-deleted-online-footprints-persist/ accessed 9 June 2018.
[1044] A bounce is when a visitor to a website only visits one page before leaving. An alternative solution could be tracing by the help of hashing.
[1045] This is also more sustainable in terms of storage and performance. Cesare Bartolini and Lawrence Siry, 'The Right to Be Forgotten in the Draft Data Protection Regulation' (2016) 32(2) Computer Law & Security Review 218, 231.
[1046] Ibid.

invalidating the originally published data makes every copy inaccessible.[1047] A combination of these two measures could be an efficient (and easy to implement) solution to guarantee the enforcement of Article 17(2).

Returning to the Google Spain case, it is interesting that the CJEU's interpretation of the right to deletion did not make any special reference to the information duty from Article 17(2), although it existed, in a limited version, under the DPD too. Nevertheless, following the judgement, Google set up two types of automatic notification procedures.[1048] The first was an automatic notification to webmasters of the URL whose removal was requested.[1049] The second was a notification system for its users.

Regarding the first type, the Article 29 Working Party stated that the communication with webmasters has no legal basis under EU data protection law.[1050] However, it may be legitimate for search engines to contact original publishers prior to any decision about a complex delisting request to gain a better understanding about the circumstances of the case.[1051] This strict approach can also be noticed in the practice of some national data protection authorities. In 2016, the Spanish DPA charged Google with a large fine for illegal sharing of deletion requests with webmasters. The DPA found that any dissemination must properly safeguard the rights and interests of data subjects. At least, this should mean that prior to any dissemination, a search engine should conclude a binding and effectively enforceable legal contract with webmasters prohibiting them from disseminating the data in an identifiable form.[1052] The arguments asserted by Google – the legitimate interest under Article 7(f) and the notification duty under Article 17(2) – were not accepted.[1053]

Moreover, Google and some other search engines have developed the practice of systematically informing the users of search engines of the fact that some results to their queries have been delisted in response to requests of an individual (the second type of automatic notification procedure).[1054] The Article 29 Working Party noted that such a practice could only be acceptable if the information was offered in such a way that users could not in any case come to the conclusion that a specific individual had asked for the delisting of results.[1055]

[1047] Ibid.
[1048] Haber, 154.
[1049] Ibid.
[1050] Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12'.
[1051] Difficult cases are those where neither of the interests in conflict seem to prevail. They often require judicial intervention. Ibid., 10. For example, the dispute in a case in which the appellant argued that Google should remove URLs that described his past criminal behavior was taken all the way up to the Dutch constitutional court (Gerechtshof Den Haag ECLI:NL:GHDHA:2016:2161 from 24 February, 2017).
[1052] David Erdos, 'Communicating Responsibilities: The Spanish DPA targets Google's Notification Practices when Delisting Personal Information' (*Information Law and Policy Centre*, 27 March 2017) <https://infolawcentre.blogs.sas.ac.uk/2017/03/27/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information/> accessed 9 June 2018.
[1053] Ibid.
[1054] Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12' (2014) 9.
[1055] Ibid.

7.4.2.2. Other types of online 'forgetting'

7.4.2.2.1. The right to object

The right to object may be invoked based on a data subject's particular situation regardless of whether the processing of her data is unlawful or not (Recital 69). The right is limited to cases in which personal data was processed because of a legitimate interest of a data controller or some public interest (Article 21(1) of the GDPR). However, if the purpose of personal data processing is direct marketing, an objection can be made at any time. As in the case of the right to erasure, 'time' can be an important factor and may tilt the balance of arguments in favour of or against recognising the right to object.[1056] As time passes, data processing may become superfluous or excessive, and it will be easier for a data subject to demonstrate her particular situation and subsequently make an objection.

Following a successful objection request, data should 'no longer be processed'. What does this mean? A hint can be found in Articles 21(2) and 21(3), which relate to the objection to using personal data for direct marketing purposes. The article indicates that even though an objection against direct marketing has been made, this same data can still be used for other reasons (e.g., billing the user).[1057] This tells us that after an objection, data is not removed from the servers. Instead, the processing is paused.

The consequences of the requirement that data should no longer be used differ from the consequences of erasure. Erasing data means removing it from the computer memory (although, as will be explained in section 7.6.2, in technological terms deletion does not necessary mean that data no longer exists). Technology offers various ways to comply with the objection. If the data is processed automatically, then the objection should be noted in the controller's IT systems. The consequence would be moving the data to a separate system, blocking the data on a website, or otherwise making the data unavailable.[1058] However, from an individual's point of view, a complete and thorough deletion is most often what is desired. After all, data that is kept on the servers for a longer time is prone to cyber-attacks and may become part of a larger, aggregate dataset that is further reused.

This limitation was seemingly acknowledged by the drafters of the GDPR, who updated the provision on the right to erasure. In Article 17(2)(c) of the GDPR, it is explicitly stipulated that objection may constitute one of the grounds to erase data.

In some cases, however, the right to object may offer more control to data subjects than the right to erasure. To illustrate the difference between the two rights in the context of the data economy, we can use the example of data shadows, i.e. information about other individuals that companies use to identify us.[1059] For example, based on the purchases of other people, Amazon recommends a book to a user. Companies typically process such data on the basis of their legitimate interests.[1060] Legitimate

---

[1056] Paulan Korenhof and others, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds) Reforming European Data Protection Law (Springer Netherlands 2015).

[1057] Article 21(3) states: '*Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes*.' *A contrario*, it can still be used for other purposes.

[1058] These technological measures were suggested as possibilities to restrict data processing as defined in Article 19, but in a non-temporarily version they can be also used to facilitate the right to objection. Bird & Bird (2017).

[1059] Digital shadows are information about others that companies use to identify us. Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice' 230.

[1060] Lokke Moerel and Alex van der Wolk, 'Big Data Analytics under the EU General Data Protection Regulation' (2017) 12 <https://ssrn.com/abstract=3006570>.

interest is a legal basis for data processing that can be used in the cases in which the interests of a controller prevail over the interests or fundamental rights of the data subject.[1061] If someone wants to delete data shadows by applying the right to erasure, he may be unsuccessful as nothing unlawful occurred, no consent was needed for the processing to start with, and the data was in principle neither irrelevant nor inadequate. The right to object, however, is still possible as long as the data subject proves that this is appropriate in his particular situation.[1062] In fact, since the processing was carried out for the purposes of advertising, it would probably be objectionable in any case (Article 20). Thus, the right to object appears broader than the right to erasure, as it enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation.[1063]

7.4.2.2.2. Consent withdrawal

Another manifestation of the RTBF is the withdrawal of consent. Because of the assumption that every data subject has free will and is capable of validly consenting to the use of her personal data, it is also necessary that consent can be revoked.[1064] This right of the data subject derives from the right to informational self-determination, which also entails that the data subject cannot waive his right to withdraw his consent in the future.[1065] Precisely this possibility of the data subject to withdraw his consent, whenever he wishes to*, 'distinguishes "consent" from "contract" as a legal basis (ground) for the (lawful) processing of data*'.[1066]

If consent is withdrawn, processing can no longer be carried out as it lacks legal basis. The only logical consequence is for it to stop. But what does 'stopping' mean, exactly? Does it only relate to the processing of data that occurred after the withdrawal, or does it include the processing that occurred beforehand? 'In other words, does the withdrawal of consent operate as a form of revocation, with an *ex tunc* effect, meaning that all existing data collected about the person withdrawing her consent must be deleted? Or is it simply a termination, thus with an *ex nunc* effect, allowing the controller to maintain (but not process further) data already collected?'[1067] As Kosta puts it, the withdrawal is effective for the future and does not have a retrospective effect, as this would render the data processing that was based on the given consent unlawful.[1068] However, given the psychological factors, an *ex tunc* effect might be more in line with users' expectations. Ordinary users expect that following an erasure request data disappears in its entirety. As a solution, Bartolini and Siry suggested an interpretation according to which consent is revoked with retroactive effects, but the controller does not incur any liability because the data processing was based on legitimate expectations stemming from the data subject's behaviour.[1069]

[1061] Article 6 (1)(f) of the GDPR.
[1062] This is actually a solution that was suggested by the CJEU in *Manni*. In Manni, the CJEU held that the publication of personal data in a commercial register is in principle allowed in order to protect third-parties on the market. However, this general rule could be overturn, should the data subject prove that in her specific case publication disproportionality affects her privacy. See section 7.4.1.2. See also European Parliament, 'Briefing from May 2017 Contracts for the supply of digital content and personal data protection' (2017) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/603929/EPRS_BRI%282017%29603929_EN.pdf>.
[1063] *Manni*, para. 61.
[1064] For some critical views regarding individuals' (dis)ability to consent see Chapter 4, section 4.2.3.
[1065] Kosta (2013) 251.
[1066] Ibid.
[1067] Bartolini and Siry (2016) 227.
[1068] Kosta (2013) 251.
[1069] Bartolini and Siry (2016) fn 88.

In any case, a withdrawal may turn into a proper deletion (i.e., actual removal of data from computer memory) when it is followed by an erasure request.[1070] This scenario is allowed under Article 17(1)(b). From the data subject's point of view, this option leads to the highest possible degree of control. However, in the big data environment, the impact of withdrawal might be limited. Consent is not particularly popular among big data users to conduct data-driven analysis. Companies often choose some other justification of the processing, e.g. legitimate interest.[1071] As a result, withdrawal will not always be a feasible way to the RTBF.

On the other hand, when the processing is based on a data subject's consent, a withdrawal can be a challenge for big data users. The controller has to ensure that data subjects have not withdrawn their consent since the time their data was collected. Monitoring this process may be cumbersome and almost impossible if the data controller does not design specific technical mechanisms that allow for the tracking of the withdrawal of consent.[1072]

7.5. Options to operationalise the RTBF beyond the GDPR

The RTBF (including its possible substitutes, the withdrawal of consent and the right to object) is not the only strategy to eliminate electronic data. The GDPR's wide-ranging catalogue of controllers' duties contains measures that could work to achieve the same goal, e.g., the storage limitation principle, privacy by design, and the principle of purpose limitation. These solutions were already mentioned in section 3.3.2.1.2. This section explores some legal and technical measures that are not foreseen in the GDPR but nevertheless facilitate the forgetting of data. Regarding legal measures, the right to a clean slate is described in more detail. In terms of technical ones, deletion-by-default, expiration dates, obfuscation, and some other solutions are discussed.

7.5.1. The right to a clean slate

A clean slate refers to a situation in which everything bad or wrong that an individual has done in the past is forgiven or forgotten, and she can make a new start.[1073] This idea comes close to the objective of the RTBF: outdated and irrelevant data can be detrimental to an individual, therefore it should not be used. Once such data is removed, an individual has the chance of a fresh start. Koops envisioned how the right to a clean state would extend to areas outside data protection law in which people are particularly vulnerable to being unduly confronted with detrimental information about their past, e.g., bankruptcy law and juvenile justice, but also labour law, consumer law, and administrative and preventive criminal justice.[1074] These context-specific measures would be aimed at controlling how other parties can use information when making concrete decisions that affect individuals.[1075] *'This could be done in the form of limiting periods during which detrimental data can be retained, or through legal mechanisms similar to the exclusionary rule (in relation to assessing evidence in a criminal*

[1070] Kosta (2013) 92.
[1071] Centre for Information Policy Leadership (2017).
[1072] Matthias Dehmer, Frank Emmert-Streib, Stefan Pickl, Andreas Holzinger (eds) *Big data of complex networks* (CRC Press, 2017) section 8.5.2.
[1073] 'clean slate' Macmillan dictionary <https://www.macmillandictionary.com/us/dictionary/american/a-clean-slate> accessed 9 June 2018.
[1074] Ibid.
[1075] Koops (2011) 255.

procedure) and non-discrimination oversight that enhance fair decision-making about job applicants and employees, consumers, (quasi-)suspects and administrative offenders.'[1076]

To illustrate Koops' ideas, consider a situation in the context of an employment relationship. Under labour laws, one common legal basis for dismissal of an employee is continuous under-performance.[1077] In recent years, algorithmic tools have become increasingly popular to assess workers and to rank them from the most to the least capable. Those at the end of the list are at risk of being fired. Cathy O'Neil wrote about US teachers who were evaluated and many of them dismissed based on the score of an AI rating; it was then found that the algorithmic decision-making used flawed metrics and that the teachers who were dismissed were in fact doing just fine. The AI tool evaluated teachers largely on the basis of students' test scores, while ignoring how much the teachers engaged the students, worked on specific skills, dealt with classroom management, or helped students with personal and family problems.[1078]

Koops suggests that either requiring the deletion of data that could lead to a biased score or imposing some sort of overseeing of possibly unfair outcomes would prevent teachers' personal data from being used in an unfair way.[1079] Frankly, this would probably not suffice. In the era of complex AI that drives business decisions, coming to fair results will require that the system of analysis be carefully examined and perhaps changed.[1080] Only then would the unfair uses of data be blocked. If such an outcome is achieved, then it would indeed be similar to what data erasure strives for. Because only specific data uses would be impacted, the right would probably be easier to implement. Along the same lines, O'Neil suggests using more targeted laws to stop potentially discriminatory uses of data in the employment context. For instance, a genome analysis which shows that a person has a high risk of breast cancer or Alzheimer's should not result in a denied job opportunity for affected persons.[1081]

Koops' idea was proposed in 2011 before the GDPR was even drafted and before the CJEU decided on *Google Spain*. Today, his vision can probably to a large extent be realised under the data protection law framework. Nonetheless, Koops' idea remains attractive because it suggests activating mechanisms in legal areas beyond data protection law.[1082] More directed rights across legal domains could facilitate consumer decision-making and ultimately the overarching notions of individual autonomy and human dignity.[1083] Moreover, they could bring together some familiar policy agendas to provide 'good' choices/options through the alignment of the available enforcement mechanisms.[1084]

[1076] Ibid.
[1077] See for instance a provision in Slovenian Labour Law (Zakon o delovnih razmerjih), Article 89.
[1078] O'Neil (2016) 41.
[1079] Koops (2011) 252.
[1080] Compare O'Neil (2016) 332-333.
[1081] Ibid., 337.
[1082] See more on this idea in Chapter 10.
[1083] Clifford and Ausloos (2017).
[1084] Ibid.

7.5.2. Technical solutions to operationalise the RTBF

7.5.2.1. My Account by Google and Privacy Basics by Facebook

Among IT companies, Google and Facebook offer two of the probably most advanced control platforms that include some 'forgetting' options.

Google's My Account site was launched in 2016 to offer Google users centralised access to privacy and security settings across the company's services.[1085] Today, it includes things like Ads Settings (to allow more precise personalisation of the ads that Google serves to the user), Privacy and Security checkups (to check the security of a user's devices and privacy settings, such as her Google public profile), but also more complex settings (e.g., to check whether users' past YouTube searches can be reflected in automatic recommendations). The idea is to make it easier to manage and protect a user's data and privacy related to Google's many services in one destination, instead of having to visit each property individually.

What the My Account website also enables is the deletion of the entire Google account or of a specific service. In some sense, this corresponds to the aims of the RTBF as it allows users to control the availability and use of their data. For instance, a user can delete past search entries or block location tracking. Moreover, a user can delete her profile information that is used to place ads (e.g., cat-lover, cyclist, traveller). However, Google only gives access to information that users shared with Google based on consent. Information that Google processes on other bases (e.g., legitimate interest) or information that Google has enriched with other data is not accessible.

With regard to users' control over data, it must be noted that identification of an individual and anonymisation of data have fundamentally changed in the last decades. Because Google has access to a vast amount of personal data on individuals who share personal characteristics, a specific user's personal data is no longer needed.[1086] Others' data (e.g., shopping habits of someone's friends or a peer group) can be equally useful to identify individuals. Over this data, however, an individual has no redress.

Following Google, Facebook took action with its Privacy settings and Privacy Basics function, which in a similar way facilitate control over data, including deletion, but also fail on the same points as the Google solution does.[1087] The Privacy Basics function leads a user through the processes of personal data control, such as deleting his posts or untagging a photo. Actual changes are made in the settings of each user's personal Facebook webpage. To delete personal data, a few different solutions are offered. For example, users' generated content can be either hidden or deleted. While in both cases the post would disappear from the timeline, hidden posts are only blocked from being shown on the website, while deletion is carried out on Facebook's servers. With regard to users' accounts, again, two options are possible. One is the deactivation of an account, which has an effect similar to the hiding of posts. The effect can only be temporary, i.e. the account reappears after some time. During this time, users' data does not move anywhere, it is just not visible on the platform. Deletion is a more permanent

[1085] <https://myaccount.google.com> accessed 9 June 2018.
[1086] Keynote address at the OHRP Research Community Forum by dr. Julia Lane in New York (US) <https://www.youtube.com/watch?v=XDT7FnXvM58> accessed 15 June 2018.
[1087] <https://www.facebook.com/about/basics/manage-your-privacy> accessed 9 June 2018.

version of removal of data; however, it comes with some limitations. First of all, deletion is not immediate. Facebook warns that it may take up to 90 days to delete data stored in backup systems. Further, some data is not stored in the deleted account. For example, a user's friend may keep her messages after the deletion request. The deletion has no effect on such data processing. Finally, copies of some materials (for example, log records) may remain in Facebook's database. Although they are disassociated from personal identifiers (i.e., anonymised), this data can still be used by Facebook for any purpose that may emerge in the future.

Just like Google, Facebook offers less control in relation to personal data that has not been collected on the basis on one's consent. However, in the aftermath of the Cambridge Analytica scandal, Facebook decided to allow more control over this sort of information as well. The recently implemented project Clear History allows users to delete information Facebook has collected from outside sites and apps on other legal bases such as legitimate interest.[1088]

7.5.2.2. Deletion-by-default

Deletion of user data by default is a technical solution to ensure erasure becomes an inherent part of data processing. By using deletion as a default, data use becomes necessarily circular, starting with collection and ending with deletion. Deletion-by-default technologies should be designed as a data black hole where every bit of data is destined to disappear.

For instance, a deletion-by-default process was built into the popular photo messaging application Snapchat.[1089] However, Snapchat should not be seen as a role model. Although its commercial campaign was based on promoting privacy of ephemeral posts, after the successful launch of the application, it was found that Snapchat did not in fact delete the photos. Even though users no longer had access to them, the photos remained on Snapchat's servers.[1090] In addition, automatic disappearance of photos was also challenged by the activity of other Snapchat users. Frankly, this should not be surprising to Snapchat users. After all, Snapchat's privacy policy clearly acknowledged this point by warning the users that those who '*see the content you provide can always save it using any number of techniques. Keep in mind that, while our systems are designed to carry out our deletion practices automatically, we cannot promise that deletion will occur within a specific timeframe.*'

7.5.2.3. Expiration dates

The idea of expiration dates for personal data addresses the time challenge of digital remembering by determining how long information should be retained and thus remembered.[1091] Two approaches can be distinguished: the first one is the expiration date for data, the second the expiration date for consent.

[1088] Heather Kelly, 'Facebook wants to make changing your privacy settings less work' *CNN* (21 May 2018) <http://money.cnn.com/2018/05/21/technology/facebook-controls-plan/index.html> accessed 9 June 2018.
[1089] Michael L Rustad and Sanna Kulevska, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28 Harvard Journal of Law & Technology 351, 390.
[1090] See the FTC press release after reaching a settlement in which Snapchat admitted that they deceived users with promises about the disappearing nature of messages sent through the service <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were> accessed 9 June 2018.
[1091] Michael L Rustad and Sanna Kulevska, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28 Harvard Journal of Law & Technology 351, 383.

One of the first advocates for expiration dates was Mayer-Schönberger, who argued that by introducing expiration dates it would be possible to mimic human forgetting in the digital realm.[1092] This would be done by associating information stored in digital memory with expiration dates that users would set by themselves: '*Our digital storage devices would be made to automatically delete information that has reached or exceeded its expiry date.'*[1093] Technically, expiration could be done by adding additional metadata, and Mayer-Schönberger predicted that this should not be a serious hassle for technological companies, although it may intervene with their established business systems.[1094] It would, however, require some state action, a requirement to change the code, or at least strong economic pressure by consumers and/or industry.[1095]

A disadvantage of this option is that data subjects need to have the foresight to accurately set the date for potentially harmful data.[1096] Data subjects might be misinformed or fail to pick the right date, which makes the idea riskier. This problem was tackled by Roxana Geambasu and her research team at the University of Washington.[1097] Their idea was to encapsulate data such as emails, selected text in messages, or documents that are sent over the Internet. The system would create corresponding keys for decapsulation that are widely available online, but that would deteriorate over time so that the data in readable form would only be available for a certain period of time. It would thus overcome the problem of user's involvement.

A solution similar to the idea of expiration dates is the expiry of consent. It would lead to similar benefits as expiration dates for data because it would create a ground for *ex nunc* (and possibly *ex tunc*) deletion of data.[1098] However, the idea does not come without problems. Custers notes that expiry dates for consent would require much metadata, which *'may also reveal privacy preferences of data subjects, yielding less privacy rather than more privacy, as privacy preferences can be used for personalization or profiling.*' [1099]

7.5.2.4. Obfuscation

Elena Esposito argues that the idea of deleting is in contrast with the nature of AI. Algorithms do not possess the human tendency to forget: they have to be programmed to do so. By forcing a removal of some memory, however, the most immediate effect is drawing attention to it, thereby activating remembering. This can be observed when Googling a particular person who was 'forgotten by Google'. Among the results, a warning appears that some of the contents have been removed in the name of the RTBF. The obvious consequence is to increase curiosity about and interest in that content.[1100]

Esposito emphasises that classical deletion does not work with AI, therefore a new approach to forgetting is needed. She proposes to *adopt a procedure directly opposed to the practice of deleting*

[1092] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2011) 171.
[1093] Ibid.
[1094] Ibid.
[1095] Ibid.
[1096] Rustad and Kulevska (2015) 383.
[1097] Roxana Geambasu and others, 'Vanish: Increasing Data Privacy with Self-Destructing Data' *Proc. of the 18th USENIX Security Symposium* (2009).
[1098] See the discussion in 7.4.2.2.2.
[1099] Custers (2016).
[1100] Esposito (2017).

contents or making them unavailable. To reinforce forgetting in the context of AI, memories should not be erased but multiplied.[1101]

One possibility to make Esposito's idea materialise is obfuscation*,* proposed by Brunton and Nissenbaum and defined as the addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects.[1102] Like the right to delist, which focuses on reused data and attacks illegitimate secondary uses, obfuscation targets secondary data processing. The point is to prevent data from being repurposed and taken out of context.

Certainly, obfuscation is not a form of erasure but rather a sort of anonymisation. However, it has similar goals. Since in some cases erasure simply will not work, obfuscation may be a good alternative, leading to similar if not the same outcomes.

7.5.2.5. Down-ranking

Down-ranking refers to the practice of deliberately placing certain search results at the bottom of the search engine result pages. In 2018, down-ranking was used by Google to limit the effect of news coming from unfriendly Russian sources as well as to reduce referrals to illegal pirate websites.[1103] This technical solution could also work for personal data. In fact, it could become a RTBF alternative that would strike a better balance between privacy and freedom of expression. By downgrading the links with personal data, privacy of a person would still be to a large extent protected whereas the information would remain available to diligent and serious researchers, thus limiting negative effects on the freedom of expression.

7.6. The RTBF as a control affording entitlement

The goal of Section 7.6. is to assess the extent to which the RTBF affords control to data subjects in the context of the data-driven economy. While doing so, the section draws on the limits and enablers to the RTBF that were identified previously in this chapter. While the RTBF in principle functions as an enabler of data subject control, it often fails to enable control, or even limits control, due to factors stemming from three major forces: technological, economic and psychological.

7.6.1. Enablers to data subjects' control

Complex and multilevel ways of data gathering affect data subjects and their experience of control. Does the RTBF offer any redress for the black box of collected data? *Google Spain* is particularly remarkable in this regard. The judgement points out the creation of profiles by combining search results, which is a data-driven type of data acquisition consisting of both data reuse and combinations of datasets. Removal of search results prevents the creation of misleading profiles and their limitless dissemination via search engines. In some sense, erasure of search results protects individuals in the data-driven economy better than erasure of original sources, because it restricts the availability of prejudiced personas generated by an algorithm. Delisting is thus a good (though not perfect) example

[1101] Ibid.
[1102] Finn Brunton and Helen Fay Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press 2016).
[1103] Adi Robertson, 'Russia warns Google over comments about downranking government-linked news sites' *Verge* (*21 November 2017)* <https://www.theverge.com/2017/11/21/16687694/russia-google-eric-schmidt-rt-sputnik-rankings> accessed 27 December 2018.

of effective application of the RTBF that helps data subjects maintain control over data, protecting their privacy and their autonomous choice.[1104]

Another attempt to enhance data subject control is Article 17(2), in which the GDPR directly recognises that threats to an effective erasure stem from unlimited data sharing and copying by third parties. Article 17(2) stipulates that following an erasure request, controllers are obliged to inform all (the thousands of) parties with whom the data has been shared. While this duty places a burden on controllers, it does too little for actual control of data subjects and effective application of the RTBF. First, third parties can be difficult to reach. In the data-driven era, data can be acquired from multiple sources and shared widely. Identifying every single transfer of data can be challenging. Second, even if all these parties can be reached and they respond to the notification, there is no guarantee that the data at their premises will in fact be deleted. The notification duty has no impact on the actual deletion of a data source. Under this duty, data controllers are only obligated to convey the information, and have no obligation regarding actual deletion.

To avoid undesirable consequences of the uncontrollable and decontextualised data collection, and thereby enhance data subject control, some technical measures resembling the RTBF prove useful as well. For example, informational intermediaries such as Google and Facebook offer 'user control platforms' where users can adapt and delete the content that they do not like. In this way, they alone control what sort of data the platforms should have access to. For instance, they may prevent search engines from linking to their social media profile. These tools should be taken with some scepticism, however, since many of them offer less protection than the legal framework provides. Nevertheless, due to their accessibility and user-friendly interfaces, they can, to some extent, achieve goals similar to those of the RTBF.

An alternative, neutral solution is obfuscation, which is the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects.[1105] For example, obfuscation software can camouflage users' search queries and cause a deadlock in online advertising processes. While obfuscation would not erase the data, data collection and subsequent reuse would be prevented. As shown above, there is no way to find and delete all copies of relevant information, but for most users only easily discoverable information matters.[1106] Thus, the result would be, to a large extent, the same as in the case of the RTBF.

[1104] This is especially true when withdrawal of consent is the basis for erasure. The Article 29 Working Party's guidelines to the RTBF suggest that if the data subject consented to the original publication, but later on revoked his or her consent, the DPAs will generally consider that de-listing of the search result is appropriate, even though the original source has not yet been removed. Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12'.

[1105] Brunton and Nissenbaum (2016).

[1106] Meg Leta Jones, *CTRL + Z: The Right to Be Forgotten* (NYU Press 2018).

7.6.2. Limits to data subjects' control

7.6.2.1. Technological forces

The RTBF also applies to algorithmically processed personal data. However, the requirements of data deletion do not easily translate because AI neither learns nor 'forgets' in the way that humans do.[1107] Data deletion in AI contexts is much more complex. In simplified technical terms, data is not truly deleted: it is simply removed from the search index. Only once the deleted space is used again is the old data inside effectively destroyed. Unfortunately, this may take a long time, as databases often append new data rather than searching for existing free space due to performance issues.[1108] Because AI remembers and forgets differently than humans do, the issue has to be tackled in AI's own way. One proposed solution is the unlearning of algorithms, a method of 'artificial' forgetting. This method introduces an extra layer between the learning algorithm and the data upon which it is trained; this layer consists of a small number of summations.[1109] Such a design eliminates any dependency each layer has on the other and allows the system to 'unlearn' a piece of data without having to re-build the entire model and the associated relationships between data.[1110]

The situation becomes more challenging when algorithms use observed and, in particular, inferred data. Inferred data is composed of characteristics assigned to a person based on her activities and behaviour online. Often, it is inferred from a large group of (similar) users. This type of data is at the heart of data-driven algorithms as it enables predictions, which companies need for various commercial purposes. If a data subject alone requests erasure, it is unlikely that withdrawing one person's data will make much difference to a trained model and/or the algorithmic outcome.[1111] To make effective use of the RTBF to alter models, whole groups would need to collaborate explicitly or implicitly to request erasure, which is highly unlikely.[1112]

Even if we disregard the issue of the AI black box, which prevents users from obtaining any meaningful understanding of how algorithms process their information, applying the RTBF in relation to AI and other new technologies proves difficult. The first example is Google's system of the RTBF. In principle, personal data should no longer be accessible through Google searches after a successful removal request has been made. However, taking advantage of the design of Google's search engine, researchers were able to identify 30-40% of deleted URLs.[1113] As the authors warn, the same exercise could be done by hackers in a cyber-attack and could lead to data abuse.[1114]

[1107] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right To Be Forgotten' [2017] Computer Security & Law Review 8.
[1108] Ibid., 12.
[1109] Yinzhi Cao and Junfeng Jang, 'Towards Making Systems Forget with Machine Unlearning' Colombia University <http://www.cs.columbia.edu/~junfeng/papers/unlearning-sp15.pdf> accessed 15 June 2018.
[1110] 'New 'machine unlearning' technique deletes unwanted data' (*Kurzweil,* 16 March 2016) <http://www.kurzweilai.net/new-machine-unlearning-technique-deletes-unwanted-data> accessed 15 June 2018.
[1111] Regardless of all the difficulties, results of algorithmic analyses should reflect individuals' real characteristics and should therefore be adjusted dynamically to their 'personas'. In this vein see also Julie E Cohen, 'What Privacy Is for' (2012) 126 Harvard Law Review.
[1112] Lilian Edwards and Michael Veale (2017) 36.
[1113] Minhui Xue and others, 'The Right to Be Forgotten in the Media: A Data-Driven Study' (2016) 4 Proceedings on Privacy Enhancing Technologies.
[1114] Ibid.

The second example are back-ups and retained data. Modern business operations such as advanced data analytics and automated business decisions increasingly rely on backed up and archived data, including personal data.[1115] Back-ups are not only critical in terms of non-disrupted business operations but also beneficial to data subjects to have their data timely available. In the context of the right to erasure, deletion of back-up systems appears impractical and undesirable from an individual perspective, as well as technically challenging.[1116] User data are not stored within a single system. On the contrary, they are spread across multiple applications and storages, off-site and onsite, and they may be found under various forms such as emails, files, database records etc.[1117]

As a side note, forgetting personal data to prevent undesirable data-driven decisions is limited by the substantive scope of data protection law. Algorithms may use aggregated personal data that cannot be attributed to a specific human being. As Article 11 of the GDPR stipulates, data control rights are inapplicable in such cases. Although such data may still be a basis for important decisions regarding citizens, it is in principle inaccessible to the de-indexing in accordance with the RTBF.[1118]

To conclude, today's data economy is transforming into an AI economy. Both leading politician and entrepreneurs have noted that those who will gain the most control over AI in the future will control the world.[1119] To save a piece of the 'control cake' for individuals, the RTBF will hardly prove useful as it has little success in controlling inferred data and is often challenged by new technologies.

7.6.2.2. Economic forces

As shown in Chapter 2, the final step in the data value chain is acting upon discovered knowledge, *i.e.* using insights into the acquired data to draw useful decisions that can generate profit. These decisions can serve the economy and individuals well, but they can also be discriminatory, privacy-infringing, or biased.

One of the RTBF's aims is to limit the (economic) use of data that can cause damage to an individual. Limiting the scope of data use to what is relevant within a specific context should in principle decrease the risk of unforeseen and undesirable consequences of data reuse. This is essentially the reason for including the principle of purpose limitation among the grounds for the RTBF. Noisy data should be removed from data processing to avoid corrupting a dataset and contaminating interpretation. However, on an increasingly personalised Internet, almost every bit of personal data can be argued to

---

[1115] Eugenia Politou et al., 'Backups and the right to be forgotten in the GDPR: An uneasy relationship' (2018) Computer Law & Security Review: The International Journal of Technology Law and Practice, 7.
[1116] Ibid., 10.
[1117] Ibid.
[1118] Esposito (2017). However, some more recent studies suggest that AI models in some cases enable data de-anonymisation and should therefore be seen as pseudonymized data (i.e., personal data). Michael Veale, Reuben Binns and Lilian Edwards, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (July 12, 2018) 376 Philosophical Transactions of the Royal Society.
[1119] A statement of the Russian president V. Putin in a recent meeting with students. James VIncent, 'Putin says the nation that leads in AI "will be the ruler of the world"' *The Verge* (4 September 2017) <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> accessed 9 June 2018. Also see statements by French president Macron. Nicholas Thompson, 'Emmanuel Macron talks to Wired about France's AI strategy' Wired (31 March 2018) <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/ > accessed 9 June 2018.

be relevant,[1120] and it will be difficult to convince data controllers that the data should be forgotten on the ground of 'no longer being necessary for the purpose for which it was initially collected'.[1121]

7.7. Conclusions

Chapter 7 sought to answer the fourth research sub-question regarding the entitlements that data subjects enjoy under the data protection laws, the implications of the data-driven economy for these rights and the extent to which these entitlements afford control to data subjects. While this research question refers to data subject rights as a whole, in this chapter the scope was narrowed down to the right to be forgotten, exploring its scope and control-enhancing potential.

Section 7.2. described the values that the RTBF protects. It was argued that control is the underlying notion of the RTBF, closely related to both data subjects' privacy and their autonomy. Section 7.4.1. summarised the relevant case law. In *Google Spain* and *Manni*, which both preceded the GDPR, the CJEU took key steps towards a modern version of the RTBF. Besides the right to erasure, two other types of legal entitlements that aim to facilitate forgetting to afford individuals active control over data, the right to object, and withdrawal of consent, were described in 7.4.2. Section 7.5. listed some other legal and technical measures that can be used as alternatives for the RTBF. Although many of these alternatives, similarly to the RTBF, face challenges, they may prove useful in specific situations. Expiration dates transform the idea of forgetting into an *ex-ante* consideration thus solving the problem of user (insufficient) involvement. The down-ranking, focused on data processing by search engines, has the potential to strike a (better) balance between privacy and freedom of expression. The final section assessed the effectiveness of the RTBF in the context of the data-driven economy. Based on this section, two conclusions could be drawn. First, it is not the RTBF *per se*, but the technological and social surrounding that gives real control to data subjects. For instance, by creating a user-friendly interface for the RTBF, Google encouraged thousands of users to file requests to be forgotten. Second, the RTBF, like some other provisions of data protection law, loses its strength due to some distinct features of the data-driven economy, such as the tendency to reuse anonymised data.

All in all, the available RTBF infrastructure is promising but still in the making. What is necessary to move toward a more coherent system is, at the minimum, additional jurisprudence on balancing the rights in a data-driven environment and technical implementations accessible to a wider public.

[1120] Graux, Ausloos and Valcke (2012) 103.
[1121] Custers and Ursic (2016) 10.

8. DATA PORTABILITY AS A DATA SUBJECT RIGHT

8.1. Introduction

Data portability is a fluid concept that can be used in multiple contexts and defined in various manners. One possible definition is the following: 'Data portability is the ability of people to reuse data across interoperable applications.'[1122]

Data portability may pursue several objectives.[1123] For instance, it has been argued that data portability is inseparably tied to the goals of competition law.[1124] Furthermore, some recent implementations of data portability indicate that it can be used as a commercial strategy to please consumers.[1125] Finally, data portability may pursue the goals of privacy, data protection, and, as will be shown in this paper, data subjects' control over their personal data.

When data portability is guaranteed by law, it is referred to as the *right* to data portability.[1126] This is the case in the EU GDPR, which recognises personal data portability as an inherent part of the EU data protection law (Article 20). Compared to the analysis of some other data subject rights in the previous chapters, the analysis of data portability is mainly theoretical as the right has only been used since 25 May 2018. Nonetheless, taking into account some of its already known legal and practical limits, it is possible to describe most feasible ways in which the right to data portability could unfold in the future.

Chapter 8 addresses the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* In this chapter the sub-question is approached from the angle of data portability. The chapter starts with a short explanation of the historical development of the idea of personal data portability (section 8.2) and continues with a legal analysis of the provisions in the GDPR to emphasise numerous legal and practical constraints to data portability, which put limits on the application of the right (section 8.3). Specifically, section 8.4 compares the right to data portability with other data subject rights. As a right under data protection law, data portability's declared goal has been to strengthen individual control over data.[1127] However, how this control could materialise in the era of the data-driven economy remains to be seen. While there has been much discussion about data portability in relation to its antitrust angle,[1128] less is known about the ways in which individuals could make use of the right. Section 8.6 then shows that data portability is not an exclusive data protection measure but can be regulated through some other legal

---

[1122] DataPortability Project <http://dataportability.org> accessed 26 April 2018.
[1123] Alexander Macgillivray and Jay Shambaugh, Exploring data portability, (ObamaWhiteHouse.Archives, 30 September 2016) <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability> (accessed 26 January 2018).
[1124] See for instance Maurice E Stucke and Allen P Grunes, 'No Mistake About It: The Important Role of - Antitrust in the Era of Big Data' (2015) University of Tennessee Legal Studies Research Paper; Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (2013) SSRN Electronic Journal; Inge Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies between Competition , Consumer and Data Protection Law' in Bakhoum, Conde Gallego, Mackenordt, Surblyte (eds.)*, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer, 2018).
[1125] See Section 8.2.1.
[1126] In this thesis, a 'right' is understood in Jhering's sense as a legally protected interest. Munroe Smith, 'Four German Jurists. II' (1896) 11 Political Science Quarterly 278, 289.
[1127] Lynskey (2015) 263.
[1128] *Supra* n 1124.

provisions such as those in consumer protection law or intellectual property law. Finally, section 8.6. examines the degree to which data portability adds to individual control from both a theoretical and a practical perspective. Section 8.7 concludes the chapter.

8.2. How and when the idea of data portability emerged

8.2.1. Commercial initiatives

Outside the data protection law domain, data portability as a concept emerged some time ago. For example, dataportability.org (also known as The Data Portability Project) was founded in 2007 to discuss and work on solutions to unconstrain data portability.[1129] This initiative set a basis for the attempts to adopt data portability in a commercial environment.

The Data Portability Project adopted a broad definition of data portability as meaning *that '[t]he user is able to obtain her data and to transfer it to, or substitute data stored on, a compatible platform.'*[1130] This definition can be broken down into four building blocks: free data access, open formats, platform independence, and free deletion.[1131]

Following dataportability.org's initiative, some data-driven platforms implemented voluntary solutions for export of the user data they held. Among others, the project attracted some of the largest data holders, such as Google and Facebook. For example, in 2011 Google created the 'Google Takeout' tool, which allows users to export and download data from 27 of Google's products.[1132] Moreover, Facebook offered a similar web-tool for downloading user information.[1133] Facebook users all across the globe were (and still are) able to download not only the information that they shared on their profile, but also other information that Facebook held on them, including a log of their activity, which is visible to users when they log into their profiles, and information that is generally not visible to users, such as ads clicked on, IP addresses used for log-ins, etcetera.[1134]

One common denominator of the commercial versions of data portability is that they strongly resemble the right to data access.[1135] The right of access gives an individual insight into his data but does not facilitate transfers to third-party providers. In fact, many commercial initiatives fail at enabling a meaningful transfer of data.[1136] As shown above, data portability in its broadest sense[1137] includes some extra qualities, such as platform independence, meaning that users could update their data on another platform and have the updates reflected in the platform currently in use. Platform

---

[1129] Barbara Van der Auwermelen, 'How to Attribute the Right to Data portabÍlity in Europe: A Comparative Analysis of Legislations' (2016) 33 (57) Computer Law & Security Review 57, 58.
[1130] *Supra* n 1122.
[1131] Todd Davies, 'Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies' in Luca Maria Aiello and Daniel McFarland (eds), *Social Informatics: Proceedings of the 6th International Conference (SocInfo 2014),* (Barcelona, 2014) 3.
[1132] <https://takeout.google.com/settings/takeout> accessed 26 January 2018.
[1133] <https://www.facebook.com/help/405183566203254> accessed 26 January 2018.
[1134] European Commission Staff, 'Online Platforms Online Platforms - Accompanying the Document Communication on Online Platforms and the Digital Single Market {COM(2016) 288}' (2016) 37.
[1135] Art. 15 of the GDPR; Art. 12 of the DPD.
[1136] Sometimes willingly. See for example the transcript of the discussion on portability in the House of Lords on online platforms and the EU digital single market (London, 23 November 2015) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/oral/25076.html> accessed 26 January 2018.
[1137] See the definition by dataportability.org: *supra* n 1122.

independence has not been built into commercial data portability initiatives. This is not surprising: absolute data portability is difficult to achieve, in particular in highly competitive business environments. Thus, a limited version of data portability is what major data-driven companies consider a good commercial strategy, offering consumers an extra benefit while not putting their business assets at risk.[1138]

Google and Facebook were not the only adopters of data portability: it has recently been implemented in the products of some minor software providers, such as Project Locker[1139] and CozyCloud.[1140] The former offers business users a cloud repository, while the latter turns to individuals, helping them handle personal data (flows). In both solutions, data portability is facilitated by APIs. After users have chosen applications with which they are willing to share their data, an API enables a connection to those applications by providing them with users' data.[1141] This kind of data portability comes closer to the version of data portability proposed by The Data Portability Project and, as will be shown, also to the GDPR's version of the data portability right.

8.2.2. Regulatory initiatives

In the regulatory domain, personal data portability was introduced along with some other initiatives that promoted rights, abilities, and influence for users regarding their online environments and data. Building on Berners-Lee's idea of a 'bill of rights' and some other calls to strengthen individual rights online, Davies included portability in his framework of digital rights.[1142] Likewise, the Electronic Frontier Foundation, a privacy rights organisation, suggested that data portability should be a building block of 'A Bill of Privacy Rights for Social Network Users'.[1143] In 2010, the US White House launched the My Data initiative with the intent of easing data access, but also of enhancing data portability.[1144]

In 2012, the requirement on data portability was made part of a data protection law for the first time. In that year, the EC began the data protection reform by publishing the draft EU GDPR. In relation to data portability, the EC's proposal was innovative, as it suggested that data portability was introduced *'to further strengthen the control over their own data and their right of access'*. Thus, the proposal introduced a right with potentially far-reaching effects, but it came with little explanation regarding its implementation.

The proposed version of personal data portability was considered somewhat controversial. During the negotiations, EU member states often had diverging views to what data portability was or should

---

[1138] Typically, commercial versions of data portability do no fully incorporate automatic, simultaneous deletion, and rarely support interoperability of formats.
[1139] <http://projectlocker.com> accessed 26 January 2018.
[1140] <https://cozy.io/en/> accessed 26 January 2018.
[1141] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' 10 <https://ssrn.com/abstract=2933448> accessed 26 January 2018.
[1142] Davies (2014) 3.
[1143] Kurt Opsahl, 'A Bill of Privacy Rights for Social Network Users' (EFF, 19 May 2010) <https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users> accessed 11 November 2017. Also see: Lisa A. Schmidt, 'Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare' 22 (2) Cornell Journal of Law and Public Policy 527.
[1144] Kristen Honey, Phaedra Chrousos, and Tom Black, 'My Data: Empowering All Americans With Personal Data Access' (Obama White House Archives, 15 March 2016) <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access> 12 June 2018.

be.[1145] At first, it was not clear from the text of the proposal whether the right was meant as a 'lex social network'[1146] or if it concerned every instance of data processing regardless of context, including sectors such as energy and finance.[1147] Furthermore, it was not clear whether data portability meant simultaneous access and transfer, or whether it was limited to transmission between services.[1148] Similar uncertainty also arose with regard to interoperability.[1149]

As shown above, personal data portability came to life as both controversial and promising. Now that the GDPR is applicable, the uncertainty regarding the implementation of the right to data portability is an issue of concern. Recognising this problem, in 2016 the Article 29 Working Party issued guidelines on the right to data portability for data controllers.[1150] The next section outlines the legal nature of the right under the GDPR, taking into account the Working Party's views.

8.3. Personal data portability under the GDPR

Under the GDPR, the right to portability has a two-fold structure. The first component is the right of individuals to obtain a copy of their data in a structured, commonly used, and machine-readable format. The second component is that this data should be transmitted to another controller without hindrance. For reasons that will be discussed in section 8.3.2, the scope of data portability under the GDPR is highly limited. As a consequence, it falls short of what The Data Portability Project considered a right to data portability.

8.3.1. Three components of the right

8.3.1.1. 'The […] right to receive the personal data […] in a structured, commonly used and machine-readable format'

In an attempt to be technologically neutral,[1151] the GDPR does not state exactly the terms 'structured', 'commonly used', and 'machine-readable format' mean. Therefore, the scope of the right to data portability is to a large extent dependent on the interpretation of these open-ended provisions. The format in which data is transmitted is clearly of the utmost importance for the efficiency of the right to data portability. When users receive data in generic formats, for example simply as a PDF or a zip file, they often face difficulties with transmitting that data.[1152] Hence, the right format is a pre-requisite for portability.

[1145] Materials from the GDPR negotiations in the Council, fn 345 <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.
[1146] A law that is primarily or even exclusively supposed to regulate social networks.
[1147] Irion and Luchetta (2013) 68.
[1148] Spain, France, and Romania wanted data portability to mean the transmission of data from one controller to another. However, the majority of delegations saw the right to portability as a right to get at copy without hindrance and to transmit data from one controller to another controller. Materials from the GDPR negotiations in the Council, fn 345 <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.
[1149] Expert Group on cloud computing contracts, 'Data Portability upon Switching' (2014) 7 <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf> accessed 13 November 2017.
[1150] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability'.
[1151] Technology neutrality means that the same regulatory principles should apply regardless of which technology is being used. In this way, the law does not render obsolete too quickly.
[1152] Expert Group on cloud computing contracts (2014) 4.

To explain the open-ended terms, some related legal documents could serve as a guideline. For example, in the directive on the reuse of public sector information, 'machine-readable' is defined as allowing software applications to easily identify, recognise, and extract specific data.[1153] Two formats that the Article 29 Working Party explicitly recommends are CSV and XML.[1154] However, even these two types of standardised formats are restricted in the sense that they do not always allow the determination of data types, primary keys,[1155] possible relationships between tables (for example foreign keys), etc., and require additional APIs to access that information.[1156]

To be 'structured', data should have a specific structure; for instance, it should be stored in a database or in specific files such as JSON or CSV files.[1157] Structured data formats not only enhance possibilities for the reuse of datasets, but also possibilities for their coupling.[1158] The latter is an integral part of large-scale data mining (data analytics).

Lastly, the data format must be 'commonly used'. The interpretation of 'commonly used' differs from industry to industry. In the music industry, completely different formats are used (for example, the MP3[1159] and AAC[1160] formats) than in the health-care sector (for example, the standardised ODM format for clinical trial data)[1161]. In some areas, common formats are determined by formal standards. In other areas, there are no common formats at all. In such cases, the Article 29 Working Party's guidelines recommend the use of open formats.[1162]

Recital 68 mentions interoperability as an additional non-mandatory requirement adding to the description of the format in Article 20. Interoperable formats enable transformation from one format to another without any loss of data. For instance, Apple's .ibooks format for ebooks can be easily transformed into the open standardised EPUB2 format.[1163] This type of format interoperability should be differentiated from a perfect technical interoperability, which requires compatibility of information systems and is explicitly exempted from the data portability provision in Recital 68.[1164]

[1153] Recital 21 of the Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, OJ L 175, 27.6.2013.

[1154] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 18.

[1155] The unique identifier of a database.

[1156] Darko Androcec, 'Data Portability among Providers of Platform as a Service' (2013) Research Papers Faculty Of Materials Science And Technology In Trnava, Slovak University Of Technology In Bratislava, 9 <https://www.mtf.stuba.sk/buxus/docs/doc/casopis_Vedecke_prace/32SN/002_Androcec.pdf> accessed 11 November 2017.

[1157] Haut, Brinkmann and Abels (2016) 55.

[1158] Bart Custers and Daniel Bachlechner, 'Advancing the EU Data Economy: Conditions for Realizing the Full of Potential of Data Reuse' (forthcoming in 2018) Information Policy 10.

[1159] MP3 is an encoding format for digital audio.

[1160] AAC is a proprietary encoding standard for digital audio compression. It was designed to be the successor of the MP3 format.

[1161] P Coorevits and others, *Electronic Health Records: New Opportunities for Clinical Research* (2013).

[1162] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 18.

[1163] Ibid.

[1164] Perfect social network interoperability (compatibility) would, for instance, enable a Google+ user to upload pictures or post messages on someone's Facebook page directly without having to create a profile on Facebook. Inge Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (2015) 39 (502) Telecommunications Policy 14-15. In a similar sense, Ian Brown argues that interoperability actually works together, or includes, interconnectivity. Ian Brown and Chris Marsden, 'Regulating Code: Towards Prosumer Law?' 24 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2224263> accessed 9 June 2018.

8.3.1.2. '[…] the right to transmit those data to another controller without hindrance'

The second dimension of the right is the entitlement of individuals to transmit their personal data from one provider to another without hindrance.[1165] The Article 29 Working Party translates the phrase 'without hindrance' into refraining from or slowing down access, reuse, or transmission. Examples of measures that create hindrance include lack of interoperability of formats, fees asked for delivering data, lack of access to a data format or API, deliberate obfuscation of the dataset, and excessive sectorial standardisation or accreditation demands.[1166]

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

Still, taking such a strong position against undesirable hindrance may be critical for the success of data portability. This has been confirmed by the efforts of the EC Expert Group on cloud computing and some international standardisation bodies that have noted a lack of interoperability and have been working on standardisation and technical solutions for data portability.[1167]

8.3.1.3. '[…] the right to have the personal data transmitted directly from one controller to another, where technically feasible.'

Data portability includes the right to have data directly transmitted from one controller to another. In line with the view of the Article 29 Working Party, the requirement can be fulfilled by making an API available.[1168] A consortium of EU digital service providers went even further, stating that 'the service provider who would not put an API to retrieve our data, while this is the most effective and cheaper to transfer data directly, would be objectively seen as trying to create friction.' Besides APIs, the use of standard protocols has been suggested as a method of direct data transfer.[1169]

According to the GPPR, a direct transfer of data between controllers is only required when technically feasible. However, what the phrase 'technically feasible' means remains open; it does not necessarily match 'operationally feasible' or 'economically feasible'. A solution proposed by the European Banking Federation (EBF) is the following: if a data controller claims that a transfer is unfeasible, it has to prove this. If it fails to do so, portability should be facilitated.[1170]

[1165] Art. 20 of the GDPR, para. 1.

[1166] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 15.

[1167] Expert Group on cloud computing contracts (2014) 7. In relation to standardisation activities of the International Organisation for Standardisation (ISO) see Irene Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology 1.

[1168] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 15.

[1169] Yunfan Wang and Anuj Shah, 'Supporting Data Portability in the Cloud Under the GDPR' 14 <http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf> accessed 12 June 2018.

[1170] European Banking Federation, 'European Banking Federation's Comments to the Working Party 29 Guidelines on the Right to Data Portability' (2017) 4 <http://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf (accessed 26 January 2018)> accessed 10 June 2018.

'To have data transmitted' implies a duty of data controllers to carry out the transmission. An alternative to assigning this duty to data controllers would be a third-party service based on an agency contract.[1171] For example, a marketing company or a data broker would offer data subjects free products or services, a voucher, or even a certain amount of money, if they authorised it to exercise their right to data portability.[1172] The company (or the broker) could later use this data itself, or sell it to interested companies.[1173] As is explained below, this model of data portability can be described as Data Portability as a Service (DPaaS).

8.3.2. The restrictive definition of the right to data portability

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

8.3.2.1. '[…] data provided'

The right to data portability only applies to data that has been provided to a controller by a data subject. First, this data includes personal data that the data subject has *actively* provided to the data controller.[1174] Examples are email addresses, telephone numbers, preferences regarding communication, etc., which the data subject typically communicates the first time she interacts with a data controller. Second, according to the interpretation of some supervisory authorities, the right to data portability also applies to data that has been provided *passively*.[1175] Typically, this is behavioural data, which has been gathered by observing data subjects' behaviour, for example raw data processed by smart meters, activity logs, history of a website, etc. ('observed data').[1176]

However, once data has been analysed using any sort of algorithmic techniques to draw useful insights, the results of this analysis should not be ported. It is arguable that in applying analytical techniques, data loses the direct connection with data subjects and is thus no longer considered to be 'provided by them'. The Article 29 Working Party refers to it as 'inferred data'.[1177] A user's profile created by the analysis of raw smart metering is one such example. Some types of data may fall between raw data and derived data,[1178] such as reputation scores that are attained by users of online marketplaces such as Airbnb. If the scores were portable, this would mean that Airbnb users would have the right to take their reviews and transfer them to a competitor, for example Couchsurfing.

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

---

[1171] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 4.
[1172] Ibid.
[1173] Ibid., subject to GDPR restrictions.
[1174] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 10.
[1175] Ibid. For a similar interpretation also see Ms Věra Jourová's letter to the WP29 chair, Ms. Falque-Pierrotin, of 4 April 2017, ref. Ares(2017)1790040 – 04/04/2017 <https://zwenneblog.weblog.leidenuniv.nl/files/2018/06/Letter-Cssr-Jourova-to-Falque-Pierrotin.pdf> accessed 27 December 2018.
[1176] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 10.
[1177] Ibid.
[1178] European Banking Federation (2017) 4.

fact, the EC criticised the Article 29 Working Party for adopting a position that was too data subject centric.[1179]

8.3.2.2. '[…] concerns a data subject'

The right to data portability is limited to data that 'concerns a data subject'. 'Concerning a data subject' means that there must be a connection between the data and the identity of an individual. Consequently, anonymous data is excluded from the scope of data portability.[1180] Moreover, Article 11(2) exempts a controller from complying with data subject rights when he is not able to identify the data subject. Thus, such de-identified data also falls outside the scope of data portability.[1181] However, if the data subject provides additional information enabling his identification, the right to data portability should again arise.[1182]

Personal data records may contain multiple persons' data, which are often intertwined. This may create additional difficulties in applying the right to data portability. When a data subject decides to transfer her social media data to a different platform, her decision may affect the data of a third party which is also part of the ported dataset. For example, porting photos of someone's friends from a closed social media network (for example, a private Facebook group) to another which is open to public by default (for example, Twitter) could infringe the privacy of this person's friends. The Article 29 Working Party adopted a strict interpretation in this regard, stating that processing of such personal data by another controller should be allowed only to the extent that data is kept under the sole control of the requesting user and is only managed for purely personal or household activities.[1183] However, in many situations, personal motives for data portability will coincide with commercial use of third-party data and will likely exceed 'purely personal or household activities'. For example, in the case of reputation scores, an Airbnb user may want to port his data to Couchsurfing, including all the reviews that he has received from Airbnb users, and may want Couchsurfing to process this data when calculating his new ratings. The Working Party's view should be taken with a grain of salt, as its purpose was not to constrain data portability, but rather to mitigate commercial exploitation of data portability.

8.3.2.3. 'The processing is based on consent […] or on a contract'

Third, data portability is only applicable in cases where the legal basis for data processing is either consent or a contract (Article 20(1)(a) of the GDPR). This provision has received some criticism, since it means that a data subject would only be able to port the data that has been processed with her approval.[1184] In other words, a data subject would have no influence over data that has been legitimately collected and processed without her consent. For example, data processing that is based on legitimate interest of a data controller is excluded from the scope of data portability. To process

---

[1179] David Meyer, 'European DPAs Mull Strategy for Tackling Uber's Data Catastrophe' (*IAPP Privacy Advisor*, 2017) <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/> accessed 26 January 2018.

[1180] Yunfan Wang and Anuj Shah, 'Supporting Data Portability in the Cloud Under the GDPR' 7.

[1181] Ibid. See also Article 11 (2) of the GDPR.

[1182] Ibid.

[1183] Ibid.

[1184] Nadezha Purtova, 'The Illusion of Personal Data as No One's Property' (2013) 7 Law, Innovation, and Technology 15. Also see Eleni Kosta and Kees Stuurman, 'Technical Standards and the Draft General Data Protection Regulation' in Panagiotis Delimatsis (ed), *The Law, Economics and Politics of International Standardisation* (Cambridge University Press, 2017).

behavioural data or to create consumers' profiles, controllers typically use the legal basis of legitimate interests.[1185] In such cases, data portability is exempted, although porting these sorts of analyses could be in individuals' interest too.[1186] Moreover, in the work environment, for example, the legal basis will almost never be consent but it will very often be a controller's legitimate interest.[1187] Therefore, the Article 29 Working Party recommended that, as a good practice, data controllers allow portability for data that is processed on the basis of legitimate interest.[1188]

8.3.2.4. '[…]the processing is carried out by automated means'

To apply the right to data portability, the processing has to be carried out by automated means. This requirement should not be read restrictively. 'The use of automated means' does not imply that there should be no human intervention whatsoever. Rather, this should be interpreted as excluding processing that is based solely on manual means.[1189]

8.3.2.5. 'The right should not apply to processing necessary for the performance of a task […] in the public interest or in the exercise of official authority […]'

This limitation comes as no surprise as it relates to those types of data processing that require either confidentiality or exclusivity. Examples include taxation, reporting crimes, humanitarian purposes, preventive or occupational medicine, public health, social care, quality and safety of products, devices and services, and election campaigns.[1190]

8.3.2.6. 'That right shall not adversely affect the rights and freedoms of others.'

Data portability should not infringe upon the right of third parties (Recital 68 of the GDPR). The right to privacy is perhaps the most obvious example. How data portability could violate a third party's right to privacy was explained above using the scenario of shared photos. Likewise, data portability should not disproportionality affect intellectual property rights.[1191] For example, it should not be possible to port copyrightable photos or other files if there is a risk that the photo may become widely shared and that the rights of the copyright owner may be appropriated.

What is less clear is whether data portability could also be restricted on the basis of the right of companies to do business (Article 16 of the EU Charter of Fundamental Rights). The first question to answer is whether this right also falls within those rights that are considered 'in accordance with the

---

[1185] Gwendal Le Grand, Jules Polonetsky and Gary LaFever, 'GDPR Data Analytics Webinar Summary Three Key Points' <https://www.anonos.com/hubfs/Whitepapers/GDPR_Data_Analytics_Webinar_Summary_Anonos.pdf?t=1507182920438&utm_campaign=Data Analytics under the GDPR&utm_source=hs_email&utm_medium=email&utm_content=57043368&_hsenc=p2ANqtz-9mifrSF5kE2AIJJGqFWy8cpF> accessed 13 November 2017.

[1186] For some examples of data analytics based on the legitimate interest of a controller see Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' 25.

[1187] Article 29 Data Protection Working Party, 'Opinion 2/2017 on Data Processing at Work'.

[1188] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' fn 16.

[1189] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 9. Article 22 adopts a stricter version of automated processing, which is made clear by using a different diction: '*solely automated [...]* '.

[1190] Andrew Cormack, 'GDPR: What's Your Justification?' *(JISC community,* 2017) <https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification> accessed 26 January 2018.

[1191] This is the limit that the GDPR mentions (Recital 63) with regards to the right to access but can be applicable to the right to data portability as well.

GDPR,' as required by Recital 68. If it does, then Article 16 of the Charter could lead to some further limits to data portability. For example, it could be argued that data portability should be restricted if it could have some major negative consequences on the business process (e.g. excessive implementation cost).[1192]

8.4. Data portability v. other data subject rights

As was already illustrated in some of the previous chapters,[1193] data subject rights are in an interplay with each other. Data portability has the closest connection with the right of access and the RTBF. Moreover, data portability is also related to the right to information. How the three rights interrelate is discussed shortly below.

8.4.1. The right of access

The right to data portability differs substantially from the right of access, although the latter can be seen as a sort of predecessor. As a first step, data portability allows for access to data, but then it goes beyond mere accessibility and insights into the data, and opens up the possibility of data transfers and potential further data use. Data portability requires data controllers to assist data subjects in taking control over their personal data and allocating a copy of the data to a party where it can be reused in the most beneficial way. This is done by mandating the use of structured and machine-readable formats, and by enabling direct transfers of data. The right of access does not come with these additional requirements which are crucial to facilitate a transfer. In some limited cases, accessing data in a commonly used format could also lead to some sort of portability, but it would certainly be a less effective option, as it would require strong personal involvement of an individual user. On the other hand, if interoperability of the systems fails, data portability is degraded to nothing more but access.

8.4.2. The right to erasure (the RTBF)

From an individual's point of view, data portability has been described as a safeguard to informational self-determination by giving the individual the freedom to choose the service provider for the storage and processing of such data.[1194] However, this freedom comes with one important limit. After data has been ported to the controller that is, in the data subject's point of view, the most trustworthy, privacy-friendly, or preferable for any other reason, a copy of it remains with the first controller.

Portability of digital data may give a false impression that it has similar consequences as portability of physical data which is withdrawn from one place and transferred to another. Digital portability does not work this way. Instead, a copy of original data is maintained and processed further on the original controller's premises, unless a data subject applies his right to erasure.[1195]

To effectively control data processing, portability will have to be enforced together with the right to erasure,[1196] so that data and not a copy of it move from one controller to another. Only when it is

---

[1192] However, accoring to the CJEU decision in *Google Spain* the right to privacy and data protection would in most cases prevail over the right to conduct business (para. 81). For a different view compare AG Jääskinen's opinion in the same case (para. 132).
[1193] See for example section 5.1.
[1194] Zanfir (2016) 4.
[1195] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 7.
[1196] Article 20 of the GDPR implies this option: '*The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17.*'

merged with the right to erasure does data portability enable full control over the processing of the data subject's personal data.[1197]

Nonetheless, the right to data portability should not prejudice the limitations of the right of the data subject to obtain the erasure of personal data, in particular when they are necessary for the performance of a contract (Recital 68). The limits of portability and erasure will have to be considered by the controller on a case-by-case basis.

8.4.3. The right to information

The initial communication with a data subject has to include information about possible remedies, including data portability. The Article 29 Working Party recommends that data controllers always include information about the right to data portability *before* any account closure.[1198] This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated.[1199] In addition, the Article 29 Working Party recommends that the receiving controllers inform data subjects about the nature of personal data relevant for the performance of its services.[1200] This allows users to restrict the risks for third parties and limit the amount of data to what is necessary (also to be in line with the data minimisation principle).

To control personal data, data subjects will always have to take some active steps that can be daunting. Being aware of the possibility to port the data is just the first step, but it may be helpful in making data subjects more aware of the reasons why data portability is desirable. For example, because a data subject dislikes the manner in which his data is used on a social network platform (e.g. political advertising), he may have a strong incentive to apply the right to data portability and start using an alternative social network instead. While it is paradoxical that the burden of discovering *ex post* opportunistic behaviour remains with the party least able to discover that behaviour – namely, the consumer[1201] – clear and understandable information can at least help make a data subject aware of her option to use data portability as an efficient remedy.

8.5. Data portability in other legal fields

In addition to privacy and data protection, data portability has several other objectives. This makes it an interesting legal concept as it fits many regulatory areas. Data portability fits competition law when its aim is to facilitate competition on the market; it fits consumer protection law when it prevents consumers from becoming entirely subordinated to powerful data service providers; and it fits intellectual property law when it aims to protect users' online creations. In this sense, data portability is also an excellent example of how multi-faceted the regulation of the data economy has become.

Data portability can be ensured in two ways: first, in an *ex ante* manner through regulatory intervention in different legal areas; and second, in an *ex post* manner through antitrust enforcement.[1202] The

[1197] Zanfir (2016) 4.
[1198] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 13.
[1199] Ibid.
[1200] Ibid.
[1201] Jan Whittington and Chris Jay Hoofnagle, 'Unpacking Privacy's Price' (2012) 90 North Carolina Law Review 1367.
[1202] Damian Geradin, 'Data Portability and EU Competition Law' (*Presentation at the BITS conference*, 2014).

GDPR's provision is an example of the first method. In addition, data portability can also be embraced *ex ante* by consumer protection and/or contractual law.

Given the multiple regulatory options, it makes sense to ask ourselves whether data protection law is in fact the best placed to regulate data portability. Some believe that making data portability part of data protection regulation is indeed a step forward, in particular because of specific normative values it brings in.[1203] Others argue that portability was appropriated by data protection law by its nature.[1204] In Koops' view, data portability would be more at home in the regulation of unfair business practices or electronic commerce, or perhaps competition law—all domains that regulate abuse of power by commercial providers to lock in consumers.[1205] *'Framing such power abuse as a data protection problem leads to introducing new types of protection into an already complex system, leading controllers to lose sight of the forest of data protection's rationale for the trees of rules, and requiring supervisory authorities to expand their staffing and scope with expertise that already exists with competition and consumer supervisory authorities.'*[1206] This dilemma is not limited to the scholarly discussion. During the GDPR negotiations, member states representatives mentioned several possibilities of where portability could be regulated: consumer, competition, data protection, and IP law.[1207]

Data portability finds itself in the conundrum of the rights-based and economic objectives. The precise relationship between these objectives remains contested.[1208] In the following sections, three manifestations of data portability in different legal domains are described. These three manifestations may also contribute to the distinct goal of data portability, that is data subjects' control over their personal data.

8.5.1. Data portability as a competition law measure

Competition law cases, both in the US and in the EU, indicate that portability of personal data could emerge as a result of antitrust policy (*ex post* portability).

In the EU, an actual or constructive refusal to enable personal data portability might constitute an abusive refusal to supply or to grant access to an essential facility, or even unlawful tying.[1209] Similarly, the US law prohibits a dominant firm from engaging in exclusionary conduct.[1210] The two systems are thus similar; however, the US law prohibits not only actual conduct but also any attempt at such conduct.[1211]

The question of data portability raised in two antitrust cases related to the processing of data on social media networks. The first case, Facebook v. Power Ventures, comes from the US. In this case, the social

[1203] Zanfir (2016) 4.
[1204] See for instance Koops (2014) 11.
[1205] Ibid.
[1206] Ibid.
[1207] Materials from the GDPR negotiations in the Council, fn 345 <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.
[1208] Lynskey, 'Aligning Data Protection Rights with Competition Law' (2017) London School of Economics (LSE) Research Online, 4.
[1209] Ibid, 12.
[1210] Van der Auwermelen (2016) 66.
[1211] Ibid.

media giant Facebook sued Power Ventures, a third-party platform, for scrapping user information from Facebook and displaying it on its own website. Facebook framed this as a copyright infringement. Power Ventures, in its counter claim, argued that Facebook was actually abusing its dominant position by *refusing its users to access their data* via a third-party platform (among others, Power Ventures).[1212] In other words, Power Ventures argued that Facebook refused to allow for *personal* data portability and therefore abused its monopoly position. In the end, the US court rejected these counterclaims and confirmed Facebook's allegations.[1213]

In the EU, the EC's investigation of Google could lead to the first 'portability case'.[1214] The proceedings against Google were initiated on 14 July 2016 and are still ongoing.[1215] Already in 2012, the Commission investigated agreements between Google and partners of its online search advertising intermediation program.[1216] Google made it highly burdensome to transfer the ability to manage ad campaigns to alternative platforms.[1217] Among others, it imposed high costs of recreating advertising campaigns, and contractual and other restrictions that may lead to the exclusion of equally efficient competitors from the online advertising market.[1218] One issue of this ongoing investigation of Google for abuse of dominance was the portability of data from Google's AdWords platform to competing online advertising platforms.[1219] To resolve the competition law concerns in relation to blocked data portability, Google proposed that it would cease any written or unwritten obligations in its AdWords API terms and conditions that hindered advertisers from transferring and managing search advertising campaigns.[1220] The EC has not yet closed this case, but its past actions indicate that it would not hesitate to consider data portability restrictions as competitive infringements.

At issue in these two cases was the competitors' right to data portability, rather than that of data subjects. Still, the two cases can serve as a useful illustration of how the goals of personal data portability and competition policy interact. To put it simply, portability mandated by the authorities distributes control over consumers' data, which in turn leads to more competition.[1221] The same happens when data subjects exercise the right to data portability. Switching between providers and avoiding locking in data portability's role enables consumers to exercise choice, an important goal of antitrust policy, which goes hand in hand with a competitive market. Hence, data portability is instrumental to the goals of competition law.

In terms of innovation progress, data portability could lead to two opposing results: it could significantly strengthen innovation by making data more available, but it could also hamper innovation

---

[1212] Ibid.
[1213] What is very interesting about this judgement is that the defendant argues his case by describing the lack of users' control and explaininig how their company's business contributes to improving the situation.
[1214] Lynskey (2017)12.
[1215] 'The Commission decided to initiate antitrust proceedings against Google's mother company Alphabet in case AT.40411' <http://ec.europa.eu/competition/antitrust/cases/dec_docs/40411/40411_15_3.pdf> accessed 12 June 2018.
[1216] 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 European Journal of Law and Technology 1 <http://ejlt.org/article/view/546>, pp.11-12.
[1217] Nathan Newman, 'Search, Antitrust and the Economics of the Control of User Data' (2014) 31 Yale J. on Reg., 63.
[1218] Lynskey (2017) 4.
[1219] 'Commission seeks feedback on commitments offered by Google to address competition concerns' <http://europa.eu/rapid/press-release_MEMO-13-383_en.htm> accessed 12 June 2018.
[1220] Vanberg and Ünver (2017) 11.
[1221] Maurice E Stucke and Allen P Grunes, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (2015) *University of Tennessee Legal Studies Research Paper*.

by making data too available.[1222] Availability of data to everyone could limit the possibilities for exploiting the economic potential of big data and thus impede innovation in the sector.[1223] Engels suggests that data portability should be interpreted in a nuanced fashion such that it does not paralyse the highly dynamic and evolving big data market.[1224] By introducing numerous exceptions and limitations, the GDPR follows this advice.

In spite of multiple interactions between data portability in the GDPR and competition law, the two instruments should not be considered substitutes. Due to its limited scope, the right to data portability can only be applied to personal data that is provided by a specific person. As a consequence, in some cases that would require data portability, such as reputational profiles on sharing economy platforms, competition law may be the only remedy.[1225] Competition law can thus work in some areas where data protection law, due to its limited scope, cannot.

On the other hand, the GDPR's right to data portability could achieve what antitrust law is not capable of doing. By applying the GDPR, it is possible to impose data portability regardless of the actual dominance of the original data controller.[1226] From this perspective, data portability has a broader scope.

8.5.2. Data portability as another aspect of the right to access industrial data

As explained above, the competition authorities have not yet shown much willingness to consider data portability as part of competition policy. However, the EU economy's need for more data portability, or in broader terms mobility, has been pressing. Data mobility is essential in achieving one of the EU fundamental goals: the free flow of personal data across the EU.[1227] This goes for both types of data, personal and non-personal.

Data mobility can be inhibited by legal, contractual, or technical measures – anything that prevents users and processing services from porting the data.[1228] Consider this example: a farmer owns a field that is being monitored via a satellite system. The satellite collects data and sends it to the storage system of the satellite system user. Can a farmer use the longitudinal data about the growth of the

---

[1222] Barbara Engels, 'Data Portability among Online Platforms' (2016) 5 Internet Policy Review Journal on internet regulation 1. Also pointed out by Google during the Enquiry in the House of Lords report on online platforms and the EU digital single market from 23 November 2015
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/oral/25076.html

[1223] Ecommerce Europe, 'Position Paper Privacy and Data Protection; Safety and Transparency for Trust and Consumer Centrality' <https://ecommerce-europe.eu/app/uploads/2016/07/ecommerce-europe-position-paper-privacy-and-transparency-for-consumer-trust-and-consumer-centricity.pdf.pdf> accessed 12 June 2018.

[1224] Ibid.

[1225] Vanberg and Ünver (2017) 2; Lynskey (2017) 20.

[1226] Ibid.

[1227] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry Reaping the Full Benefits of a Digital Single Market' [2016] COM(2016) 180 final 15
<http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15267>. Also see: Herbert Zech, 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 Journal of Intellectual Property Law & Practice 460.

[1228] Commission, 'The Proposal for the Regulation on a framework for the free flow of non-personal data in the European Union' COM(2017) 495 final, 12.

crops?[1229] Is the satellite system obliged to grant him this right? Today, firms engage in 'trading' and 'sharing' data based on contract law without legal recognition of data ownership.[1230] This means that the satellite system will typically use standard contract terms to determine the possibilities to access data and/or its alterations. If the satellite system is proprietary, the terms will typically be formulated in a way that protects private interests. For instance, the terms could assign an exclusive right to data use to the satellite system and limit the access to data by the owner of the field.[1231]

Such contractual clauses could harm the companies that cannot control data but indeed have interest in accessing it. Since competition law is not of much help when a company that controls data is not dominant and because personal data portability does not apply for aggregated data, the Max Planck Institute recommended a version of data portability with a broader scope.[1232] The EC seemingly agreed. In January 2017, the Commission published a draft regulation of the free flow of data which acknowledged the importance of the portability right for the further development of the digital single market.[1233] The proposal does not create a new right of porting between data storage or other processing service providers but relies on self-regulation for transparency on the technical and operational conditions relating to data portability. This soft measure is in line with the outcomes of the public consultation on the free flow of data that took place in 2016, where many respondents expressed hesitation in relation to a binding right to industrial data portability.[1234]

Besides this general portability provision, some other sector-specific regulatory initiatives also encourage portability of data. In the banking sector, the revised payment services directive imposes an obligation for banks to enable third-party providers to manage their clients' finances.[1235] In the near future, consumers may be using Facebook or Google to pay bills, make money transfers, and analyse their spending, while still having their money safely placed in their current bank account.[1236] Under the payment services directive, banks are obliged to provide these third-party providers access to their customers' accounts through open APIs.[1237] This will enable third parties to build financial services on top of banks' data and infrastructure and stimulate the data market even more.[1238] As a result, the

[1229] For the purposes of this tekst, let us assume that the data set includes peronsal data, e.g. moves of the farmer across the fields.
[1230] See more in section 4.3.4. on property rights in relation to data.
[1231] Contrary to such commercial agreements, the EU funded Copernicus project has a more flexible data reuse policy. For their terms see <https://scihub.copernicus.eu/twiki/pub/SciHubWebPortal/TermsConditions/TC_Sentifnel_Data_31072014.pdf> accessed 12 June 2018.
[1232] Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition on the European Commission's " Public Consultation on Building the European Data Economy "' <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf>.
[1233] *Supra* n 1228.
[1234] <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy> accessed 15 June 2018.
[1235] Directive 2015/2366/EU 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, OJ L 337/35.
[1236] Viola Hellström, 'PSD2 - the directive that will change banking as we know it' (Evry) <https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/> accessed 12 June 2018.
[1237] Ibid.
[1238] Ibid.

economy could benefit from a more competitive economic environment, and consumers could benefit from more choice and less entrenched data.

8.5.3. Personal data portability at the intersection between consumer and data protection

The discussion on the antitrust objectives of data portability in section 8.5.1. focused on the economic (im)balance between companies and, to a limited extent, between companies and consumers. For competition policy, the latter is relevant in terms of consumer choice as long as it is linked to the competition on the market. However, the (im)balance between companies and individuals seems to play a larger role in consumer protection policy. Data portability could decrease imbalances and enhance consumer protection by, for example, (a) creating a more user-friendly online environment in which the users would trust, and (b) allowing users the freedom to choose the service that best suits their needs (e.g., that is more privacy safe).[1239]

Data portability demonstrates that consumer protection and data privacy objectives are strongly intertwined. In the US, these two policies have traditionally been considered jointly under the powers of the same federal agency, the US Federal Trade Commission (FTC). In March 2012, the FTC issued a report in which portability was highlighted as one of the key privacy-enhancing policy measures that should be applied in the scope of a broader consumer protection policy. Similarly, the EU is moving its privacy and consumer protection policies closer to each other. Kerber notes that many issues that are brought up and legally challenged by data protection supervisors use reasoning that closely resembles that in consumer policy: *'Therefore, it is not surprising that to a large extent also the same policy solutions are discussed as, e.g., more transparency about the collection and use of data or limiting the collection of data, offering more privacy options, or rights to facilitate the withdrawal of data or data portability.'*[1240] Chapter 3 already discussed some of the overlaps between these two legal domains.

Recently, the link between consumer protection and data portability has been brought to light in the proposal for the directive on digital content (DCD).[1241] This directive addresses problems such as consumers' weakened position in the digital economy and the issue of elusive digital ownership.[1242] In Articles 13 (2)(c) and 16(4)(b), the DCD proposal mandates that consumers be given the option to retrieve their data for free when they leave a service. These provisions are broader than those of Article 20 of the GDPR. Data portability is not only required with respect to personal data, but also with respect to any other content provided by the consumer and any data produced or generated through the consumer's use of the digital content.[1243] Under the DCD version of data portability, the right would

---

[1239] Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> accessed 12 November 2017.

[1240] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection and Data Protection' (2016) <http://www.uni-marburg.de/fb02/makro/forschung/magkspapers/index_html%28magks%29> accessed 12 June 2018.

[1241] 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.

[1242] For a detailed study of this issue see: Jason Schultz and Aaron Perzanowski, *The End of Ownership; Personal Property in the Digital Economy* (The MIT Press 2016).

[1243] Ruth Janal, 'Data Portability - A Tale of Two Concepts' (2017) Volume 8 JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 59 <https://www.jipitec.eu/issues/jipitec-8-1-2017/4532/JIPITEC_8_1_2017_Janal.pdf>.

apply to, e.g., pictures uploaded by the consumer as well as to the online photo album which he created online.[1244]

8.6. The right to personal data portability as a control affording entitlement

Following the example from the previous three chapters, section 8.6. explores whether the right to data portability under the GDPR is actually enhancing data subject control. To this end, the sections below discuss a number of enablers and limits to the right. Special attention is given to the implications of the data-driven economy for the right. Contrary to the analysis of enablers and limits to data subject rights from previous chapters, the chapter at hand takes a more theoretical approach. The reason is that the right to data portability is new to the body of data protection law and has had, to date, only limited application.

8.6.1. Enablers to data subjects' control

As already mentioned in the introduction, the most (if not the only) plausible reason why data portability has become part of the GDPR is that it also aims to achieve the GDPR's goals of privacy and data protection. More specifically, portability of data strengthens data subjects' control over their data. Recital 68 of the GDPR sends a clear message: *'To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller'.*[1245]

In spite of this endorsement of data portability as a control-enhancing right, the recital itself has little substance with regard to *how* data portability enables data subject control over personal data. Similarly, Article 20 is silent about the specific control-enhancing functions of the right to data portability. That said, these functions can be distilled from the GDPR as a whole. They are:

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

The sections below explore each of the functions and discuss the extent to which they enable data subject control.

8.6.1.1. Control over personal data transfers

At its core, data portability is a rule about data transfers. A transfer (migration) of data should happen in an organised manner, in line with data subjects' preferences. As the Article 29 Working Party explains, data portability guarantees the right to receive personal data and to process it according to the data subject's wishes.[1246] For example, the data subject may opt for a more privacy-friendly service

---

[1244] Ibid.

[1245] Although Commissioner Almunia has also clearly acknowledged that data portability is also a measure of competition law. Joaquín Almunia, SPEECH-12-860: Competition and personal data protection (Brussels, 26 November 2012) <http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> accessed 23 January 2016.

[1246] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 5.

provider, for example Wire[1247] instead of Skype.[1248] While doing so, she might wish to ensure that all her contacts, conversation history, and chat groups are transmitted to this new provider.[1249]

Data 'porting' can be done in different ways. The choice between the alternatives foreseen by Article 20 of the GDPR has further implications for the level of control that a data subject is able to exercise. Two possibilities are:

- A transmission of the overall dataset, or extracts of it; and
- A transmission using a tool that allows extraction of relevant data.[1250]

The second option enables the data subject to opt for portability of a limited set. As a result, the receiving controller only receives the data that is needed for a specific activity or task. As this method prevents bulk data transmission, it helps guarantee compliance with the principle of data minimisation.[1251] If portability is approached in this way, then it is indeed possible to agree with the Article 29 Working Party's statement that *'[d]ata portability can promote the controlled and limited sharing by users of personal data between organisations …'*[1252] At the same time, a data subject is given a more precise and meaningful overview and control over the personal information.

8.6.1.2. Enabling control over (re)uses of data

Data portability helps data subjects exercise control not only over data transfers but also over direct future uses of data. More specifically, the right to data portability has the potential to enable individuals to use data to create value.[1253]

For example, individuals could either use the data for their own purposes, or license the data for further use to third parties in exchange for additional services or cash value. One viable way to do this would be to derive utility from connected (IoT) devices. For instance, athletes who track their activities with a smart watch may have trouble transmitting their data from their smart watch to the provider of a data processing service, such as Strava.[1254] Data portability helps overcome the transmission hurdle. Furthermore, the athletes would be compensated for allowing their athletic performance data to be displayed and analysed on a competing platform.[1255]

[1247] Wire – a communication app offering end-to-end encrypted chats, calls, and file transfers, protected by European privacy laws.
[1248] Skype is a voice over Internet Protocol (VoIP) software application used for voice, video, and instant messaging communications. Definition from Techopedia <https://www.techopedia.com/definition/15615/skype> accessed 23 September 2018.
[1249] Simultaneously, a data subject will also have to make sure that her data gets deleted from the first controller's servers. Otherwise data portability will add little to actual control.
[1250] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 16.
[1251] Art. 6(1)(c) of the GDPR.
[1252] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 5.
[1253] 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' 13. The possibility to use data was explicitly mentioned as one of the objectives of the right of data portability in the proposal for the GDPR: 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) 1 final.
[1254] Strava is a website and mobile app used to log athletic activity via GPS tracking.
[1255] It should be noted that the European Data Protection Supervisor expressed disagreement with the possibility of monetary compensation for personal data exchange: European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content'.

Data portability can only lead to control over data reuse if it is supported by functional infrastructure. For instance, by using personal data stores, privacy dashboards or other kinds of personal data management software, data subjects could hold and store their personal data and grant permission to data controllers to access and process the personal data as required.[1256]

Hub of All Things[1257] and Inrupt[1258] are free online tools that enable users to store and manage personal data. The services pull in personal data from around the Internet to enable users to view their personal data and share it with others. A similar solution is the blockchain technology developed by Pikciochain, a Swiss software firm, which is intended to facilitate individual data sharing and even sale.[1259] According to the founders, a special quality of Pikciochain is that all data uses are perfectly traceable, thus giving the users a better overview and control over sold, shared, or ported data.[1260] Finally, the MyData initiative launched by the Finnish government is a solution that also appeals to data protection rights.[1261] The aim is to provide individuals with some practical means to access, obtain, and use datasets containing their personal information, such as purchasing data, traffic data, telecommunications data, medical records, financial information, and data derived from various online services, and to encourage organisations holding personal data to give individuals control over this data, extending beyond their minimum legal requirements to do so.[1262]

However, it should be kept in mind that many decentralised architectures for supporting privacy self-management have failed in the past.[1263] The reasons were complex, ranging from purely technical (for example, network unreliability) to cognitive (such as the incorrect assumption that users were able to exercise more control than they were actually capable of).[1264] Despite this, recent research has shown that modern privacy dashboards have been quite successful in achieving the goal of strengthening control over data flows.[1265]

In spite of the myriad of options briefly described above, companies often find it difficult to convince customers to exercise their right to data portability.[1266] As a solution, the concept of data portability as a service (DPaaS) has been proposed.[1267] In a DPaaS relationship, a data subject could authorise a DPaaS provider to exercise the right to data portability in her name and to demand that her data be sent

---

[1256] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 16.
[1257] <https://hubofallthings.com> accessed 26 January 2018.
[1258] <https://www.inrupt.com/> accessed 27 December 2018.
[1259] Regarding the possibility of selling personal data see: European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content'.
[1260] There are arguments against such a positive approach to the block chain technology but this discussion is out of the scope of this paper. An interested reader should be referred to: Michèle Finck, 'Blockchain Regulation' (forthcoming, 2018) *German Law Journal*.
[1261] Antti Poikola, Kai Kuikkaniemi and Harri Honko, 'MyData – A Nordic Model for Human-Centered Personal Data Management and Processing' <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=ibid> accessed 1 November 2017.
[1262] A similar UK initiative, which has winded down in the recent months, is the 'midata' project. See <https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment> accessed 26 January 2018.
[1263] Kristina Irion et al, 'A Roadmap to Enhancing User Control via Privacy Dashboards' (IVIR, 2017) 13-14.
[1264] Ibid.
[1265] Ibid.
[1266] Michael Röhsner, 'Data Portability as a Service; A Legal and Normative Analysis of the Requirements under the Law of the European Union for Contracts That Authorize a Service Provider to Exercise the Right to Data Portability on Behalf of a Data Subject' (Leiden University 2017) 11.
[1267] Ibid.

directly to a third party or to the DPaaS provider itself.[1268] In this way, data subjects could have their data ported and transferred to a preferable provider, while businesses would benefit from access to additional data sources.[1269]

One important question to answer in this regard is whether such contracts are in fact allowed under EU law. One possible hesitation could be that data in such contracts would be handled as a commodity, which may not be in line with the strict protection of privacy and data in the human rights laws.[1270] Furthermore, a related question is whether fundamental rights are transferable. The European Court of Human Rights has held that this is not the case.[1271] However, exercising data portability on behalf of a data subject does not require a transfer of the right: only data is transferred. The right to data protection remains intact; for example, individuals can demand deletion of data at any time (within the legally defined limits). The authorities seem to agree with this explanation. The Article 29 Working Party even foresees such relationships emerging in the future.[1272] In the past, several Data Protection Authorities have stated that it is legal for a data subject to authorise a third party to exercise the right of access in his name.[1273] This argument can indeed be extended to all other data subject rights, including the right to data portability.[1274]

8.6.1.3. Enabling control over multilevel data flows and complexity

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

At the moment, exercising the data access right can simply lead to receiving multiple pages of information.[1275] With data portability, people will be able to search within and analyse the data that organisations hold about them.[1276] Data could be ported to data analytics services, which could provide deeper insights into what information it holds. For example, individuals could examine data about particular types of activity (for example, helping them to reduce their energy usage) or data that links together different types of activity (for example bringing together their transport spend with the routes

---

[1268] Ibid.
[1269] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 16.
[1270] For an in-depth analysis see Röhsner (2017) 16-17.
[1271] See for example: European Court of Human Rights, Sanles Sanles v. Spain, App. no. 48335/99; European Court of Human Rights, Thévenon v. France, App. no. 2476/02; European Court of Human Rights, Mitev v. Bulgaria, App. no. 42758/07; European Court of Human Rights, M.P. and Others v. Bulgaria, App. no. 22457/08; European Court of Human Rights, Koch v. Germany, App. no. 497/09.
[1272] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' 19.
[1273] Austrian Data Protection Commission, Decision of the 14-12-2012, K121.897/0020-DSK/2012. See also UK Information Commissioner Office, 'The Guide to Data Protection' 49 <http://www.inf.ed.ac.uk/teaching/courses/pi/2017_2018/PDFs/guide-to-data-protection-2-9.pdf> accessed 12 June 2018.
[1274] Röhsner (2017) 18.
[1275] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' [2016] 65 <http://www.narcis.nl/publication/RecordID/oai:tilburguniversity.edu:publications%2F368e6b30-32b4-478b-be2f-b9a27ee7a072> accessed 12 June 2018.
[1276] Jenni Tennison, 'Data Portability' (*Jeni's Musings*, 2017), <http://www.jenitennison.com/2017/12/26/data-portability.html> accessed 26 January 2018.

that they travel).[1277] Thus, the right to data portability could enable greater literacy regarding how data is used.[1278]

8.6.1.4. Enabling free development of personality and equality

Data portability is a manifestation of the broader right to privacy, which is an enabler to many other rights, including the right to free development of human personality and the right to equality. [1279]

First, data portability has implications for the right to free development of human personality. This can be observed in situations where data subjects have formed an entirely new personality on the Internet, such as an account on a digital shopping platform that has built up a reputation and history. An example is a user's eBay reputation: *'A long-time seller on eBay has a reputation that she has built up carefully. But if she switches to the entrant, she will be a newbie again and buyers will naturally be reluctant to transact with her. But there is a ready solution: make the eBay identity and reputation portable. If I am a good seller on eBay as HotDVDBuysNow, I should be just as good on another site.'*[1280]

Indeed, on websites like eBay, the concepts of digital identity and reputation are fragments of the general dimension of one's identity and reputation.[1281] Both terms are strongly linked to the concept of (digital) personality. Data portability pursues the goal of free development of human personality by offering the means to achieve it, namely a technical process.[1282]

Second, the EU data protection supervisor (EDPS) suggests that data portability could also help minimise unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes.[1283] Unfortunately, the EDPS does not articulate how exactly data portability would achieve this. One could think of a situation in which a data subject may want to transfer data from an email service provider which uses personal data for behavioural advertising, for example Gmail, to a less intrusive one, such as Outlook. However, this still does not completely solve the problem of possible discriminatory data uses. Google would still be able to use historical data to use behavioural advertising on its Chrome browser.[1284] Data portability does not mean that data is entirely removed from the first controller's server: it only means that *a copy* is transferred and reused. Only in combination with the right to erasure can portability effectively prevent data-driven decision-making that could otherwise have a negative effect on the data subject. However, using the right to data portability to send data to a third party to conduct an impartial check could decrease the risk of discrimination. In the context of profiling, portability of personal profiles to trusted third parties could offer a solution to the lack of control over personal data. These third parties would examine the profiles and determine whether the decisions made based on them were erroneous, biased, or unfair. The idea

---

[1277] Ibid.
[1278] Urquhart, Sailaja and McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' 8.
[1279] Eva Fialová, 'Data Portability and Informational Self-Determination' (2014) 8 (45) *Masaryk University Journal of Law and Technology*.
[1280] Quoted from Zanfir (2016) 6.
[1281] Ibid.
[1282] Lynskey (2017) 38. It should be pointed out that portability could nevertheless be limited if third party rights would be affected.
[1283] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content'.
[1284] Gewirtz, David, 'Your questions answered: Why I switched from Outlook to Gmail' (*ZDNEt,* 7 August 2014) <http://www.zdnet.com/article/your-questions-answered-why-i-switched-from-outlook-to-gmail/> accessed 26 January 2018.

faces an important limitation: the narrow definition of the right. As data portability as a right only applies to data provided by the data subject, profiled data could hardly fall within Article 20's definition. Nonetheless, companies could allow this sort of portability voluntarily as a sign of compliance and trust.[1285]

8.6.2. Limits to data subjects' control

Subsection 8.6.1. showed that data portability, in principle, enhances protection of and control over personal data. In some situations, however, the right to data portability limits data subject control. This may occur when data portability is used for exclusively profit-generating goals. For example, some data-driven start-ups in the health-care sector have already investigated their options under Article 20 to gain access to medical data typically stored at a hospital or some other health-care service provider.[1286] In such cases, instead of individual control, the result is a new form of commercial exploitation and, as a result of wide data sharing, decreased privacy protection. Similarly, data portability limits data subject control when it enables a transfer of data from a more to a less secure data controller. Although the ability to make a transfer may give the impression of empowering data subjects, this control actually vanishes once data reaches an unreliable controller.

In addition, the right to portability is limiting because of the GDPR restrictive diction. First, the language of the provision in Article 20 is restrictive as it seeks to balance competing commercial and personal interests. Section 8.3.1. demonstrated that many types of personal data fall outside the scope of data portability. To process behavioural data or to create consumers' profiles, controllers typically use the legal basis of legitimate interests. In such cases, data portability is exempted, although porting these sorts of analyses could be in individuals' interest too. Second, portability is dependent on ICT infrastructure. More specifically, data portability is contingent on the use of interoperable formats and systems, and on the security of those systems.[1287] The success of data portability as a right will be correlated with the success of standardisation initiatives and with the robustness of information security.

8.7. Conclusions

This chapter addressed the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for them and, specifically, how do they afford control to data subjects?* The focus was on the entitlements in relation to the right to data portability.

It was explained that data portability is a new-born right with a narrowly defined scope which has consequences for its control-enhancing mission. On the one hand, data portability may increase transparency of data processing and may allow data subjects to control their online identities. On the other hand, the right to data portability in the present form is considerably limited and, at this point in time, any further regulatory changes to Article 20 are highly unlikely.

[1285] Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193.
[1286] The information is based on the series of interviews conducted by the author in May 2016 with entrepreneurs from Leiden Bio Science park.
[1287] European Banking Federation (2017) 3.

That said, the GDPR's version of data portability is not alone in the mission to enhance data subjects' control. Some other legal domains such as competition law contain similar ideas on portability that could lead to positive outcomes for individuals. In fact, taking a holistic view of data portability could therefore be a way to make the weak right ready for the challenges of the big data era while avoiding stretching the definition of personal data too far.

9. DATA SUBJECT RIGHTS IN RELATION TO PROFILING

9.1. Introduction

Chapters 5-8 all addressed the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection laws, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* By exploring the control-enhancing aspects of data subject control, the chapters showed that data subject rights address some of the most troubling issues in relation to data processing in the big data era. For example, Chapter 5 acknowledged the increasing information asymmetry and showed how the right to information and the right of access tend to bring more transparency in data use and reuse. Chapter 7 demonstrated how the right to erasure materialises the belief that people should have a mechanism to remove inappropriate data. In Chapter 8, the right to data portability was presented as an entitlement that tends to shift control over personal data back to data subjects by allowing them to transfer their data between data controllers.

In Chapter 9, the fourth research sub-question is addressed from the perspective of Articles 21 and 22 of the GDPR, more specifically the right to object and the right not to be subject to automated decision-making. To answer the research sub-question, the chapter defines their scope and assesses the extent to which they can be used as a measure to control personal data profiling and algorithmic decision-making. To provide the reader with the essential context, this chapter first explains profiling as a phenomenon akin to the modern data economy. Subsequently, it dives into the GDPR, analysing the relevant provisions through the lens of individual control. Finally, the chapter assesses the degree to which the GDPR has been successful in enabling data subjects to control profiling and automated decision-making.

9.2. Profiling as a building block of the data-driven value chain

As was explained in Chapter 2, the mechanisms of the data-driven economy can be broken down into three crucial phases: data collection, data analysis, and data-driven decision-making. In business terms, these three steps are referred to as 'the data value cycle (chain)'.[1288] Certainly, this is a simplified illustration which often does not match reality.[1289] Nonetheless, it is useful to understand the role of profiling in the data economy.

9.2.1. The definition of profiling

Although profiling relates to all three steps in the data value chain, it is most closely connected to the second step, the analytics. For the consumer-oriented industries that depend on analytics of their user data, profiling is a way to thrive on the competitive market.[1290] For example, data-driven profiling is the backbone of the growing online advertising sector. Google and Facebook, both known for their sophisticated profiling methods, capture over 80% of the worldwide spend in the sector.[1291]

[1288] OECD, *Data-Driven Innovation* (2015) <http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en> 32-33.
[1289] For instance, the decision-making stage could be replaced with another round of data collection, followed by an additional data analysis, before a final decision would be taken.
[1290] Pasquale (2015).
[1291] Jillian D'Onfro, 'Google and Facebook extend their lead in online ads, and that's reason for investors to be cautious' *CNBC* (20 December 2017)

Furthermore, consumer profiling is spread widely across the financial sector. A study found that 13 of the top 15 banks and credit unions that sell insurance products through their financial consultants profile their customers, as do 9 of the top 10 institutions that sell insurance through licensed platform bankers.[1292]

Hildebrandt's description is a good starting point to define profiling. Hildebrandt defines profiling as the process of 'discovering' correlations between data in databases that can be used to identify and represent an individual or group, and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.[1293] Hildebrandt's definition implies that data profiling happens after the data has been collected in a database and before any concrete business decisions or measures have been taken on its basis. This means that data collection is the input for profiling and that the business decisions are its output. What happens in between is a complex analytical process that can be in principle be broken down into two large sub-processes: 1) discovery of correlations to create a digital identity (a profile) of an individual or of a group, and 2) application of the profile to either depict an individual or to link her to a group of similar individuals.[1294]

Based on Hildebrandt's definition, profiling should be used as an umbrella term for (at least) four subcategories:

- creation of a group profile (*e.g., women in Leiden are blonde, tall, smart);*
- creation of an individual profile *(e.g., an insured person's name, address, past employment(s), payment history, etc.*);
- application of an individual profile to depict this individual *(e.g., based on her paying history, she is an unreliable person)*
- application of a group profile to identify somebody as a member of a group *(e.g., based on Amazon purchases of other people, person X should be recommended book Y).*[1295]

What does not appear clear from Hildebrandt's definition is the predictive nature of profiling. Profiling generates stereotypes by assuming that certain characteristics (receiving good grades from a prestigious university) predict certain behaviour (securing a well-paid job).[1296] This sort of stereotyping or predictive profiling is particularly apparent in the application of a group profile to an individual in the fourth bullet point. It allows the most complete use of available data, as it can be used to predict someone's behaviour and character, to attribute specific risks to her (so-called scoring), and to act towards her in specific ways.[1297]

<https://www.cnbc.com/2017/12/20/google-facebook-digital-ad-marketshare-growth-pivotal.html> 13 June 2018.

[1292] Margarida Correia, 'Customer Profiling: The Secret to Top Bank Life Insurance Programs' Financial Planning (28 May 2015) <https://bic.financial-planning.com/news/customer-profiling-the-secret-to-top-bank-life-insurance-programs> accessed 13 June 2018.

[1293] Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Gurtwirth Serge (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 41.

[1294] Paul De Hert and Hans Lammerant, 'Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever?' in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *B Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 146-148.

[1295] Hildebrandt (2008) 43.

[1296] Frederick F Schauer, *Profiles, Probabilities, and Stereotypes* (Harvard University Press 2006) 6.

[1297] De Hert and Lammerant (2016) 147.

Predictive or indirect profiling is the category of profiling that this chapter primarily considers. To illustrate its application in practice, three examples are given below.

Profiling in insurance: Car insurance companies deploy profiling to calculate their customers' risk of being involved in an accident. The higher the risk is, the higher the premium will be. To assess the risk, they want to know what their customers do for a living, where they live, their age, and their marital status. This in itself is informative, but since it also works as a proxy to consumers' lifestyle and behaviour,[1298] it can be even more revealing. For instance, a person's address can work as a proxy for his race or religion, if he lives in a neighbourhood with a Muslim majority population. Consumer's profiles are typically compared with the scores of other consumers based on the data held by the insurance company itself or licensed from other data providers. Comparing data from multiple consumers allows the insurance company to place a consumer in a category and assign a premium accordingly. Such insurance profiling may lead to discrimination: it was shown that people living in mostly black neighbourhoods were assigned higher premiums than those living in the white ones, although the differences in their personal situation or driving skills were negligible.[1299]

Profiling in an election campaign: In the 2016 US election campaign, Cambridge Analytica (CA) conducted massive profiling of US voters. After having thousands of Americans complete its survey, the company developed a sophisticated psychographics model which enabled it to predict the personality of every single adult in the US and identify the most convincing political message/ad for each potential voter.[1300] By using publicly available sources (e.g., social media, data brokers, etc.), CA acquired over 5,000 data points on each US voter. This enabled it to predict, with a stunning probability, the psychological characteristics of (potential) voters. Leveraging this newly acquired knowledge, the profiling significantly boosted Ted Cruz's candidacy and helped calibrate his message.[1301] Voters who were influenced by the use of CA's artificial intelligence were typically unaware of the impact and possible harms of such political profiling.[1302]

Profiling and the IoT: A smart home is a typical example of an IoT environment. To work properly, smart-home devices collect data and make inferences on a regular basis. For example, they check whether a user is home yet so that the temperature can be adjusted in a timely manner.[1303] In other words, smart devices constantly carry out profiling of their users, predicting what their reaction should be based on the data that the users share with them. The Nest brand thermostat collects data such as current temperature, humidity, ambient light, and whether something in the room is moving. Based on this data, Nest not only automatically adjusts the temperature but also makes inferences about the presence and specific location of occupants in a home, their current state (e.g., asleep or awake), and

---

[1298] David Edmonds, 'Does profiling make sense - or is it unfair?' *BBC News* (19 December 2017) <http://www.bbc.com/news/stories-42328764> accessed 13 June 2018.
[1299] Nest Privacy policy, active as of November 1, 2017 <https://nest.com/ca/legal/privacy-statement-for-nest-products-and-services/> accessed 13 June 2018.
[1300] Presentation of Cambridge Analytica, 'The Power of Big Data and Psychographics' <https://www.youtube.com/watch?v=n8Dd5aVXLCc> accessed 13 June 2018; Lili Levi, 'Real "Fake News" and Fake "Fake News"' (2018) 16 First Amendment Law Review, forthcoming.
[1301] Ibid.
[1302] Dipayan Ghosh and Ben Scott, 'Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You' Time (19 March 2018) <http://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/> accessed 25 August 2018.
[1303] Wachter (2017) 14.

other aspects of home activity.[1304] Moreover, the Nest thermostat may share this data with a connected car, say a Tesla, to help predict the time of a user's return from work.[1305] In fact, the wide sharing of data between devices in addition to data proliferation is a key feature of IoT. IoT-driven profiling may simultaneously and inadvertently lead to intrusion into users' privacy. Consider a user who spends a significant amount of time at home or in a shopping mall. The absence of regular working hours can be a proxy for unsteady working relationships and may indicate future defaults on loan.[1306] As a result, such a person may experience difficulties obtaining a credit card or may even be denied one.

9.2.2. Data science methods used for profiling

Data science is a broad term referring to various methods of working with data.[1307] In recent years, it has seen unprecedented advances. New data science methods are capable of coping with vast and unstructured databases. This allows them to model complex non-linear correlations in social phenomena. In comparison to older data analytics methods, the new models reach a level of accuracy that is considerably more operationally useful.[1308]

As already mentioned in section 2.2.4., one of these quickly developing analytical techniques is machine learning (ML).[1309] ML incorporates knowledge of computer science, statistics, AI, and information theory.[1310] It focuses on designing algorithms that can learn from and make predictions on the data. A specific feature of ML is that output and input variables are both fed into an algorithm, which is how the algorithm 'learns'.[1311] Learning algorithms are particularly suitable for profiling purposes, as profiles are patterns resulting from a probabilistic processing of data.[1312] Therefore, it comes as no surprise that the developments in analytical techniques have led to an increased use of profiling.[1313] ML can be particularly useful in IoT environments. Among others, ML has been recommended as a technique for predictive maintenance of smart devices,[1314] improving their speech recognition,[1315] and enabling hand-based activity recognition.[1316] Furthermore, in our current

[1304] Ibid.
[1305] Lauren Hepler, 'Ford, Nest, the Internet of Things: Can mobility merge with smart energy?' *GreeBiz* (28 January 2015) <https://www.greenbiz.com/article/ford-nest-internet-things-can-mobility-merge-smart-energy> accessed 12 June 2018.
[1306] Crootof, 23.
[1307] Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee, 'Introduction' in Mak, Tjong Tjin Tai and Berlee (eds) *Research Handbook Data Science & Law* (Edward Elgar, forthcoming 2018) 2.
[1308] Lilian Edwards and Michael Veale (2017) 6.
[1309] Kamarinou and others (2016) 4.
[1310] Atkinson JA and others, 'Combining Semi-Automated Image Analysis Techniques with Machine Learning Algorithms to Accelerate Large-Scale Genetic Studies' 6 GigaScience 1.
[1311] Lilian Edwards and Michael Veale (2017) 6.
[1312] Ibid.
[1313] Recording of the MIT 6.0002 class: Introduction to Computational Thinking and Data Science <https://www.youtube.com/watch?v=h0e2HAPTGF4> 20 February 2018.
[1314] Lynne Slowey, 'Improving operations with IoT and predictive maintenance' (*IBM*, 9 May 2016) <https://www.ibm.com/blogs/internet-of-things/improving-operations-iot-predictive-maintenance/> accessed 20 February 2018.
[1315] George Anders, 'Alexa, Understand Me' MIT Technology Review (9 August 2017) <https://www.technologyreview.com/s/608571/alexa-understand-me/> accessed 20 February 2018.
[1316] GM Weiss and others, 'Smartwatch-Based Activity Recognition: A Machine Learning Approach' *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (2016).

interconnected, data-driven society, ML systems have demonstrated the ability to automate difficult or nuanced tasks such as search, machine vision, and voice recognition.[1317]

All this considered, ML and some related sophisticated analytical techniques have some significant disadvantages. Due to their complexity, these systems are difficult to understand, explain, and scrutinise. They operate in an opaque way and are designed to work autonomously. Who would expect that someone's credit score could be determined on the basis of location data collected by his own car? All these characteristics of the IoT systems may create challenges for transparency, explainability, and human intervention, which are all, as will be shown, requirements under the GDPR.

9.2.3. Risks of profiling

9.2.3.1. Possible harms

The knowledge that is derived from data with the help of profiling is no absolute truth. On the contrary, it is likely that inferences are partial, based on inadequate data, or simply non-causal.[1318] Such profiling leads to decisions that negatively influence consumers and other individuals.

In fact, profiling can represent a serious threat to some fundamental values and legal interests.[1319] Two major negative side effects are discrimination and invasions of privacy.[1320] The former is related to lack of fairness, whereas the latter links to opacity and power asymmetries of data processing. In the first profiling scenario in section 9.2.1, people living in the neighbourhoods with a high percentage of Afro-American inhabitants were assigned higher premiums. For an algorithm, someone's postcode is a neutral piece of information, yet it can work as a proxy for race and thus lead to discrimination. In the IoT scenario, the proliferation and sharing of data out of context contributed to privacy violations. Through the combination of data, the AI was able to predict the person's unemployment and negatively influence her creditworthiness.

Other negative effects are loss of autonomy, one-sided supply of information, and risks to democratic values.[1321] In the case of Cambridge Analytica, a campaign used a sophisticated advertising strategy to target potential voters. While aggressive advertising is an inherent part of every election, the new combination of technology and big data generated knowledge on human psychology puts voters in a vulnerable position.[1322] What is particularly worrying is the failure of information to circulate freely, which could undermine voters' active right to vote.[1323]

[1317] Lilian Edwards and Michael Veale (2017) 7.
[1318] Choong Ho Lee and Hyung-Jin Yoon, 'Medical Big Data: Promise and Challenges' (2017) 36 Kidney Research and Clinical Practice 3.
[1319] See section 2.4.2. for more information about possible harms in the data-driven economy.
[1320] Bart Custers, 'Data Dilemmas in the Information Society' in Custers B.H.M. and others (eds), *Discrimination and Privacy in the Information Society* (Springer 2013) 1.
[1321] Ibid. Due to the limits of scope, profiling related harms will not be considered in more detail. An interested reader should be referred to e.g., Custers (2004); Serge Gutwirth and Mireille Hildebrandt, 'Some Caveats on Profiling' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (2010) <http://www.springerlink.com/index/10.1007/978-90-481-8865-9> accessed 13 June 2018; Lyon (2007); Zarsky (2002).
[1322] Ginger Zhe Jin, 'Artificial Intelligence and Consumer Privacy' (2017) <http://www.nber.org/chapters/c14034> accessed 13 June 2018.
[1323] The European Court of Human Rights: Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights: Right to free elections (updated 30 May 2018) 21 <http://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf> accessed 24 February 2018.

Potential violations of these rights and interests seem sufficiently serious to warrant some legal protection. As is shown in the following sections, the right to object to profiling and, in some cases, the right not to be subjected to profiling represent two such legal safeguards.

9.2.3.2. Profiling with no human intervention – the real danger?

When profiling is carried out as part of an automated decision-making process with no human involvement, additional concerns may arise. An example is issuing a speed ticket based on someone's licence plate number. After cameras record that someone has exceeded the speed limit, they report it to a monitoring system, which then issues a ticket to the owner of the car. One risk is that it was not the owner but his wife who was driving the car when the speed limit was exceeded. This may lead not only to charging the wrong person, but also to revelations of private matters. As is shown below, the legislator considered such solely automated decision-making as particularly risky and imposed some further restrictions on it. Notably, Article 22 represents such a safeguard.

In essence, Article 22 requires that automated decisions that have significant effects on individuals must either not be taken, or must encompass human supervision. A normative argument that supports the legislator's stance is the following: if the decision-making process becomes fully automated, there is a risk that an individual could become an object of a solely computing exercise. Consider the following example of a hate speech detection algorithm. In 2015, Twitter deployed AI to identify online terrorists and their advocates. Besides suspending the accounts of the users who could actually be linked to terrorism, the AI also deleted the accounts of all women named Isis.[1324] The algorithm was not able to distinguish the word 'ISIS' in different contexts but simply eliminated all the accounts, causing emotional and material damage to affected women. Along these lines, Hildebrandt refers to privacy as protection of the 'incomputable self'.[1325] Incomputability is not a rejection of machine learning, but rather a rejection of the assumption that its output defines humans.[1326]

An additional argument in favour of an increased scrutiny on solely automated decisions concerns the excessive trust in AI. Technological companies in particular seem to trust their AI tools unlimitedly, describing them as '100x more reliable than humans'.[1327] As this excessive trust drives the development of even more autonomous systems, a stringent approach seems appropriate.

However, the combination of AI and human intervention does not necessarily decrease the risk. The story of the profiling system COMPAS is telling. In that case, US judges used an AI system to assess defendants' recidivism.[1328] Although these AI analyses were not binding for judges but only served as recommendations, they proved decisive for the final judgement.[1329] This case implies that the policy of

---

[1324] Elle Hunt, '"Facebook thinks I'm a terrorist": woman named Isis has account disabled' *The Guardian* (18 November 2015) <https://www.theguardian.com/technology/2015/nov/18/facebook-thinks-im-a-terrorist-woman-named-isis-has-account-disabled> accessed 12 June 2018.

[1325] Mireille Hildebrandt, 'Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning' (2018) 33 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081776> accessed 10 June 2018.

[1326] Ibid.

[1327] <https://www.oracle.com/database/autonomous-database/feature.html> accessed 20 February 2018.

[1328] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, 'Machine bias: There's software used across the country to predict future criminals. and it's biased against blacks' *ProPublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 12 June 2018.

[1329] '*These tools may impact how judges, prosecutors, and court staff exert their own discretion, even if they don't perceive a difference*.' Angèle Christin, Alex Rosenblat and Danah Boyd, 'Courts and Predictive Algorithms' <http://www.law.nyu.edu/sites/default/files/upload_documents/Angele Christin.pdf> 2.

imposing additional legal rules for solely automated decision-making may be based on shaky grounds. The results produced by a machine, using increasingly sophisticated software and even expert systems, have an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating her own responsibilities.[1330] Hence, the combination of a human and AI judgement can be as problematic as a solely automated decision.

The following section shows how EU law distinguishes between the rights that individuals have in relation to solely automated profiling and those that they have in relation to profiling which is supervised by humans. Notably, the right to object applies in the latter case.

9.3. How the GDPR tackles profiling on the individual level

9.3.1. The GDPR's definition of profiling

For the first time in the history of EU data protection law, the GDPR has provided a definition of profiling. According to Article 4, *'"profiling"' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.'*

Given the serious threats that profiling imposes and its imminent presence in the modern economic environments, putting down a definition should be welcomed. However, it does not come without problems. In fact, regulation of profiling has many disadvantages in common with data protection law, such as the broad scope and the challenging choice between legal bases.

When trying to clarify the definition, one thing is almost impossible to miss: the diction is somehow circular. Profiling is defined as *processing of personal data* consisting of the *use of personal data* to evaluate individuals. The phrase '*use of personal data*' was not part of the EC's proposal.[1331] The insertion in the adopted version of the regulation gives an impression that the move was deliberate. The legislator might have wanted to avoid overly wide interpretations of profiling that would include, for instance, creation of group profiles composed of anonymised data. Instead, the legislator wanted to shift the focus to the application phase, i.e., when the aggregated data is used to assess individual personal characteristics. This is when the 'processing of personal data' starts and when personal data is put at risk.[1332]

[1330] Mendoza and Bygrave (2017) 7, quoting a European Commission's decision from 1990.

[1331] 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2017) 6.

[1332] The focus on the application phase resembles a system that regulates data use rather than data collection. The idea of such system has been advocated in the US: *'…the problem is that the collector has the power to curtail your freedom. Whether they use it or not, the fact that they have that power over us is itself a harm.'* Bruce Schneier, 'Nissenbaum on Regulating Data Collection and Use' (Schneier on Security, 20 April 2016) <https://www.schneier.com/blog/archives/2016/04/helen_nissenbau.html> accessed 12 June 2018. In the EU this view was not particularly well received: '*When the question of legitimacy shifts to the question whether some defendable use could be made of personal data in the future, however, much personal data collection easily becomes legitimate in a world of Big Data.'* Van Hoboken (2016) 248.

The focus on personal data is understandable. EU data protection law is fundamentally linked to the processing of personal data.[1333] As long as personal data is used, the GDPR applies. If data processing, for instance the creation of a group profile, does not involve the processing of data relating to identifiable individuals, the protection against decisions based on profiling does not apply. Some authors argue that using anonymised personal data on a group level is as problematic as applying it to individuals (or even more).[1334] In Floridi's words, '*[t]he observed is moved to an observer's local space of observation (a space which is remote for the observed), unwillingly and possibly unknowingly. What is abducted is personal information, even though no actual removal of information is in question, but rather only a cloning of the relevant piece of personal information.*'[1335] For instance, the use of big data on a group level (e.g. genetics) can inform decisions about the overall future increase in insurance premiums and risk stratification.[1336] It seems plausible that the de-identified members of a group have a stake in how they are perceived and how the research modifies the group's identity.[1337]

Regardless of how severe the risks of anonymous data processing could be, these issues are in principle not a matter of data protection law. Admittedly, it is not the task of data protection law to resolve all the problems of the emerging data technology. Instead, the focus should be on effective protection of individual privacy and personal data. Therefore, the situations in which a decision-maker merely attempts to profile data subjects without arriving at the evaluation stage would seem to fall outside the scope of the definition.[1338] In fact, Article 22(1) of the GDPR seems to presume that the decision will ultimately involve processing of data on that person as the right/prohibition it lays down is *operationalised* by reference to the 'data subject'. [1339]

However, since in the big data age almost every bit of anonymous information can be linked to a bit of personal information, which in turn de-anonymises the former, data protection law may in fact apply to an extremely wide range of information. Drawing on the CJEU jurisprudence, Purtova claimed that in Europe even weather can be considered personal data.[1340] However, such wide application is not recommendable, as it results in high and sometimes unnecessary compliance cost, and offers little extra protection to individuals.[1341]

9.3.2. The difficulties with asserting the legal basis for profiling

As any other data processing, carrying out profiling requires a legal basis. Out of the seven legal bases recognised under the GDPR, the most common ones in the context of profiling are consent, contract, and legitimate interest.

[1333] Bart Schermer, 'Risks of Profiling and the Limits of Data Protection Law' in B. Custers et al (ed), *Discrimination & Privacy in the Information Society* (Springer 2013), 48-49.
[1334] Linnet Taylor, Luciano Floridi and Bart van der Sloot, *Group Privacy: New Challenges of Data Technologies* (Springer 2017).
[1335] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 483.
[1336] Ibid.
[1337] Ibid.
[1338] In particular, the authors point at the emission of the phrase '*intended to evaluate*'. Mendoza and Bygrave (2017) 13. Also see Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017) 19.
[1339] Mendoza and Bygrave (2017) 7, quoting a European Commission's decision from 1990.
[1340] Purtova (2018).
[1341] Gerrit-Jan Zwenne (2013) 8.

When controllers rely upon consent as their legal basis for profiling, they must bear in mind that, to be valid, consent has to be freely given, specific, informed, and unambiguous (and explicit in the case of special categories of data).[1342] Given the nature of profiling, it may be difficult to collect or to give *specific* consent.[1343] Profiling is often based on analytical techniques such as data mining which have the objective of finding implicit and previously unknown relations between data. Therefore, providing a detailed description of the processing of data in advance is often impossible. In cases when profiles contain sensitive data (such as health, racial, or other sensitive data), consent must be explicit.[1344] In all other cases, regular consent is sufficient. However, organisations are able to identify special categories of data (sensitive personal data) as a result of the profiling of ordinary data.[1345] For example, it is possible to infer someone's state of health from the records of his food shopping combined with non-personal data on the energy content of foods.[1346] In this way, the explicit consent requirement can be easily bypassed. In addition, consent should be free. This means that it cannot be used as a basis for profiling in environments where power imbalances often occur (e.g., a workplace).[1347] Finally, consent should be informed. However, as profiling is often opaque and lacks transparency, providing informed consent is often challenging.

Considering these multiple drawbacks of consent, it is not surprising that the GDPR itself has indicated that consent should not be an exclusive basis for profiling by offering the option of two other bases which are legitimate interest and contract.[1348] Lee believes that *'[there is] … an express acknowledgement, directly within the operative provisions of the GDPR, that profiling can be based upon these non-consent-based processing grounds - establishing objectively and definitively that, as a matter of law, consent is not required for all profiling.'*[1349]

The first alternative to consent as a legal basis are contracts. Such contractual relationships could be primarily seen in domains such as insurance, education, employment, finance, online sales, and advertising.[1350] Data processing can be agreed upon in a contract if it is *necessary* for its performance.[1351] In the GDPR, the phrase 'is necessary' appears several times. 'Necessity' implies the need for a combined, fact-based assessment of the effectiveness of the measure for the pursued objective and of whether it is less intrusive than other options to achieve the same. Thus, in the context of profiling, a contract can only be used as a legal basis if the profiling is necessary for the execution of the contract and no other, less intrusive measure is available to the parties of the contract. This strict approach certainly narrows the scope of situations in which contracts could be used as a basis. There are few agreements for which profiling will prove indispensable. One such example is profiling in the

---

[1342] UK Information Commissioner Office, 'Feedback Request – Profiling and Automated Decision-Making' 13 <https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf> accessed 12 June 2018.
[1343] Ibid.
[1344] Phill Lee, 'Let's sort out this profiling and consent debate once and for all' (*LinkedIn Pulse,* 4 July 2017) <https://linkedin.com/pulse/lets-sort-out-profiling-consent-debate-once-all-phil-lee/> 20 February 2018.
[1345] Ibid.
[1346] Ibid.
[1347] Article 29 Data Protection Working Party, 'Opinion 2/2017 on Data Processing at Work'.
[1348] Article 21(1) referring to Article 6(1) (e), (f).
[1349] Phill Lee, 'Let's sort out this profiling and consent debate once and for all' (*LinkedIn Pulse,* 4 July 2017) <https://www.linkedin.com/pulse/lets-sort-out-profiling-consent-debate-once-all-phil-lee/> accessed 20 February 2018.
[1350] Emre Bayamlıoğlu, 'Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation' (2018) 13 <https://ssrn.com/abstract=3097653> accessed 22 May 2018 .
[1351] GDPR, Article 22(2)(c).

insurance sector, where the entire business is dependent on the comparison between the customers and overall risk assessment.

The other alternative to consent as a legal basis, the legitimate interest, is arguably the most feasible option. Legitimate interest could serve as a justification in a wide range of cases of profiling such as personalised communications, targeted advertising, business intelligence, ad performance, and audience measurements.[1352] When asserting their legitimate interest, data controllers must be able to demonstrate that the profiling is necessary to achieve that purpose, rather than simply useful.[1353] This brings us to the balancing test between commercial interests of data controllers and privacy interests of data subjects. If controllers fail to show that their interests prevail (which will not be an easy task given the human rights dimension of data subjects' interests), they need to turn to an alternative legal basis. For example, location data processing is critical for the functioning of location-based services on mobile devices. If these devices cannot readily determine location in urban environments or indoors, the service becomes useless. Because of that, it should be possible to collect location data on the basis of legitimate interest. However, this same data can also be used to build a profile on the data subject for marketing purposes – to identify her food preferences, or lifestyle in general.[1354] This further use of the location data may not be compatible with the purposes for which it was initially collected, and may thus require a different legal basis such as consent.[1355]

9.3.3. Individual rights in relation to profiling

In general, the GDPR consists of two types of provisions: those addressed to individuals and those addressed to data controllers.[1356] When it comes to profiling, the former stand on the front line and form some of the most novel parts of the GDPR. This is not to suggest that controllers' obligations are irrelevant for profiling. On the contrary, profiling is explicitly mentioned as an important aspect to be kept in mind during a privacy impact assessment (Article 34 GDPR). Nevertheless, the section below focuses on individual rights and their relevance for profiling. Only when appropriate and necessary, the focus briefly shifts to consider controllers' obligations as well.

9.3.3.1. Hildebrandt's choice architecture

Two rights in the GDPR explicitly refer to profiling. These are the right to object (Article 21 GDPR) and the right not to be subject to automated decision-making (Article 22 GDPR). Hildebrandt has noted this unique characteristic of the two rights. Together with the right to information, to the extent that it refers to automated decision-making, she grouped them in a joint cluster of rights. This cluster is referred to as a 'choice architecture for data subjects'.[1357] Choice architecture is a term drawn from the behavioural economics literature and refers to the organisation of the context in which people make decisions. It can help users to feel in control and nudges them towards decisions in their interest.

[1352] Centre for Information Policy Leadership (2017) 26.
[1353] UK Information Commissioner Office, 'Feedback Request – Profiling and Automated Decision-Making' 13.
[1354] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017) 18.
[1355] Ibid. As noted by Article 29 Working Party, this would also be in conflict with a data subject's privacy expectations. Namely, the data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late.
[1356] Although the GDPR as whole is, ultimately, addressed to both groups of actors.
[1357] Mireille Hildebrandt, 'No free lunch' - Presentation at the NIPS Symposium 'Machine Learning and the Law' in Barcelona, Spain on 8 December 2016 <http://slideplayer.com/slide/12090618/> accessed 13 June 2018.

The rights in relation to profiling resemble the choice architecture to the extent that they help users stay in control over their personal data and nudge them to (re)consider possible negative consequences of profiling.

Admittedly, Hildebrandt's choice architecture cluster is not the only part of the GDPR that can be useful to control profiling.[1358] Some other rights that have not been mentioned above can be useful too. For instance, the right of access helps individuals gain extra information about automated decision-making during the course of data processing.[1359] The RTBF provides additional control by allowing a data subject to require erasure of profile data.[1360] Finally, the right to restriction of processing is another useful and welcome form of redress in the context of unlawful profiling techniques.[1361]

As mentioned above, all three provisions that constitute the 'choice architecture' contain an express reference to profiling and/or automated decision-making. This is an interesting angle from which the three rights can be analysed. As the right to information has already been examined in detail in Chapter 5, the remainder of this chapter focuses on two other rights: the right to object and the right not to be subject to automated decision-making.

9.3.3.2. The right to object

Under the right to object, individuals may, on grounds relating to their particular situation, object to the processing of their personal data (Article 21 GDPR). As the GDPR now explicitly stipulates, under Article 21 individuals may also object to *profiling*.

The GDPR names a right to 'object to' rather than a right to prevent or stop the processing in question, but it is clear that the latter is intended.[1362] Article 21(3) explains that following a successful objection, the personal data should no longer be processed. When the processing ceases, the data does not vanish: it is just no longer available for any sort of operation performed on personal data.[1363] However, since the objection under Article 21 is a gateway to the RTBF,[1364] the data can eventually be permanently deleted. The only condition is that the right to object has been successfully exercised.

The right to object exists regardless of whether the processing at issue causes harm or is prejudicial in some way to the data subject.[1365] The standard to trigger the right to object is low and has a subjective

---

[1358] Kaltheuner and Bietti note that the rights to erasure and restriction of processing could be useful and welcome forms of redress in the context of unlawful profiling techniques. '*In contrast to the portability rights established in Article 20, Articles 17 and 18 apply to all personal data, not just those that have been provided by the data subject.'* However, further guidance is needed to clearly set out the Article's scope of application. Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2017) 2 Journal of Information Rights, Policy and Practice.

[1359] See Chapter 6.

[1360] See Chapter 7.

[1361] This right was excluded from the scope of thesis. An interested reader should refer to Kaltheuner and Bietti (2017) 16.

[1362] Frederik J Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' (University of Amsterdam 2014), 216.

[1363] Article 4(2) on the definition of processing. As the definition of processing includes storage, 'no longer processed' should equal 'no longer stored' which would in turn indicate proper removal of data. However, this was not the regulator's intention as otherwise it would not have foreseen erasure for the data in relation to which the right to objection was applied.

[1364] See Article 17(1)(c).

[1365] Robert C Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of The Public Sphere' (2014) 67 Duke Law Journal 981, fn 60.

nature as it refers to the grounds relating to someone's particular situation.[1366] This situation can be something that is irrelevant to the majority of data subjects but proves critical for the data subject in question. In this way, the right to object offers a context-aware and individualised assessment which is applied to the circumstances of the data subject's objection. Individualised harm is particularly relevant in relation to profiling. Companies that use profiling and big data are able to hold users liable for their own behaviour and for the actions of those in their networks. It has been shown that this may have particularly negative impacts on the poor.[1367] An increased insurance premium may not cause much harm to a wealthy person but it can be a significant burden for a person living on the edge of poverty.

The right to object is an important manifestation of the fairness principle in Article 5(1)(a) of the GDPR. Through objecting, data subjects are empowered to *ex post* challenge the legitimacy of the *ex ante* balancing test.[1368] The *ex ante* test is conducted before the data processing starts to ensure its lawfulness. The purpose is to help controllers assess whether the processing of data that they are about to start is in fact necessary.[1369] Furthermore, the link with the notion of fairness is confirmed by the fact that the right to object requires data controllers to balance their legitimate interests in data processing with the interests or fundamental rights and freedoms of individuals (Article 21 (1)) before they reject an objection.[1370]

The right to object is limited to cases in which profiling or other use of data is based on legitimate interest or when it is necessary for the performance of public functions, the exercise of official authorities, or a task carried out in the public interest.[1371] Hence, when consent or a contract is used as a legal basis, the right to object does not apply. In the case of consent, this is not an issue. After having consented, the data subject maintains the right to withdraw, which has similar consequences as an objection. On the other hand, if a contract is used as a legal basis, there is no such alternative. The reason is perhaps that contracts are mostly entered into in the areas of finance or insurance. In those areas, individual objections to profiling on solely subjective grounds are not viable as they could lead to abuses. Nonetheless, this limitation is remediated by the fact that a data subject may still invoke her other rights, e.g., the right not to be subjected to automated decision-making, or use alternative mechanisms in contract or consumer protection law.

Furthermore, the right to object cannot be upheld in cases in which the *ex post* balancing test shows that the legitimate reasons of a data controller prevail over the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defence of legal claims. It may be the case that the

---

[1366] The DPD contained a different standard – namely 'compelling and legitimate ground'. In comparison to the GDPR standard, it tended to be somehow objective. The UK and Irish laws specified that by expounding that processing '*is causing or likely to cause substantial damage or stress'* to a data subject or to another person and that the damage or distress was unwarranted. This precise explanation resulted in a higher bar for data subject objection requests. Ustaran and International Association of Privacy Professionals (2012) 135.

[1367] Law Review and others, 'Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans' (2017) 95 Washington University Law Review 53.

[1368] I.e., the balancing that happens at the initial data collection when possible legal basis are assessed. Clifford and Ausloos (2017).

[1369] Article 6(1) of the GDPR.

[1370] Data Protection Network, 'Guidance on the Use of Legitimate Interests under the EU General Data Protection Regulation' 8.

[1371] Italy, Denmark, Austria and Luxembourg extended the right to basically all circumstances and included all legal basis for data processing. Korff (2002) 112.

profiling is beneficial for society at large (or the wider community) and not just for the business interests of a controller, such as profiling to predict the spread of contagious diseases.[1372] The burden to set up and carry out a balancing test is placed on data controllers.[1373] Article 23 of the GDPR lists a number of additional exemptions to the right to object, such as research and public safety.

Notably, the right to object has one subcategory: the right to object to *processing for the purposes of direct marketing.* This category is not limited by the legal basis of data processing and does not require a balancing of data subjects' particular reasons for objection. As a result, the application of the right is essentially absolute.[1374] The bar for objections is set at a low level because direct marketing[1375] is considered one of the most severe interferences with data subject privacy. Whatever the circumstances, the data subject should be able to object to processing. It should be kept in mind that '*processing for the purposes of direct marketing'* is a wider notion than '*direct marketing'* only. It encompasses both the placing of the ads and the preparatory phase, such as the creation of a consumer profile.[1376] Both activities thus fall under the right to object in Article 21 of the GDPR.

The right to object applies to all types of data processing, including the processing of electronic communication data. The latter is additionally regulated in a specific legal act, namely the ePrivacy directive.[1377] In principle, the GDPR and ePrivacy directive are aligned. For example, where Article 13 of the ePrivacy directive provides a right to object to unsolicited communications, e.g. to block unsolicited calls and e-newsletters, it also refers back to the GPDR.

As part of the right to object, controllers are now required to present the possibility to invoke the right clearly and separately from other information (Article 21(4) GDPR). This express reference to objection forms part of the profiling-related choice architecture, intended to nudge data subjects to more conscious and controlled decisions regarding their personal data. However, facilitating the process of invoking the right to object does not solve all the problems. Two remaining issues are a) how to make data subjects aware of the (undesirable) data processing, and b) how to encourage them to actually apply the right to object. As profiling is often opaque, it is difficult to note when certain data processing is in fact problematic and objectionable. Transparency is of special importance in such cases.[1378] The GDPR stipulates that in the context of the use of information society services, the data subject may exercise his right to object by automated means using technical specifications (Article 21(5)). Like many other GDPR provisions, this provision is open to interpretation. One feasible way to implement the

---

[1372] Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' 52.
[1373] Article 29 Working Party's suggests that the controllers would '... at *least consider the importance of the profiling to their particular objective; consider the impact of the profiling on the data subject's interest, rights and freedoms – this should be limited to the minimum necessary to meet the objective; carry out a balancing exercise.*' Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679'.
[1374] However, transparency alone may have important limits in the world of big data. For a critical view see Hacker and Petkova (2017).
[1375] Today, all marketing really is direct marketing. Modern brand and consumer relationships are now built on greater insight, heightened personalisation and ever-more direct sophisticated marketing. This is achieved through the intelligent collection and analysis of data that has become available as consumers spend more time connected via multiple devices. Obviously, such an approach involves a lot data reuse. <http://www.theguardian.com/media-network/marketing-agencies-association-partner-zone/2015/may/20/modern-direct-marketing-data-analysis> accessed 23 January 2016.
[1376] Moerel and van der Wolk (2017) 28.
[1377] *Supra* n 397.
[1378] Gabriella Cattaneo and others, 'European Data Market SMART 2013 / 0063 D8 — Second Interim Report The Data Market in the World' 160.

right to object is to integrate it with data processing. In the context of social networks, this would work in a similar way as the 'Why am I seeing this ad?' and 'I don't like this ad' functions, enabled by social media providers for each ad that has been placed on the timeline. Data subjects could point to an ad that they find problematic for any reason and remove it instantly. Another option would be to implement the right as a privacy tool on a user's dashboard. This may not be as obvious, but seems less annoying.

9.3.3.3. The right not to be subject to solely automated decisions

9.3.3.3.1. The prohibition

Article 22 of the GDPR provides the right for data subjects not to be subject to a decision that produces legal effects concerning them or affects them significantly and that is based solely on automated processing of data intended to evaluate certain personal aspects. This provision can be read in two different ways: either as a right that the data subject can exercise, or as a prohibition for data controllers.

Under the EU data protection directive, which contained a highly similar provision, the authorities' views on its interpretation differed.[1379] The latest opinion by the Article 29 Working Party made it clear that the provision has a prohibitory nature.[1380] In other words, data subjects do not need to act to prevent automated decision-making, but are rather protected by default. Supervisory authorities should bear the burden of enforcing Article 22 of the GDPR by ensuring that automated decision-making is carried out legally, and could levy penalties and fines in cases of illegal decision-making.[1381] In the same vein, the prohibition should be considered a *positive obligation for* data controllers to guarantee protection to data subjects. Placing a prohibition that requires no individual action but rather conduct from a data controller in the section on data subject rights teaches us an important lesson on the limitations of data subject control. In some situations, and especially in an automated environment, it is best to shift control to controllers rather than expect data subjects to actively invoke their rights. The Article 29 Working Party's description of Article 22 GDPR as an example of individual control 'par excellence' is thus puzzling, as the prohibition is essentially a recognition of the inherent limits of data subject control.

Article 22 of the GDPR is likely to become increasingly important, particularly given the trend towards the convergence in technologies, increasing amounts of data linking to individuals, and the widening of the concept of personal data to include less traditional identifiers such as IP addresses, biometrics, and GPS data.[1382] Moreover, Article 22 of the GDPR has the potential to curtail the increasingly widespread use by businesses and government agencies of automated methods for categorising, assessing, and discriminating between persons.[1383] On a more normative level, Article 22 aims to infuse fairness into automated decision-making processes, ensuring that all data processing operations are indeed 'fairly balanced' for each data subject.[1384] As such, Article 22 explicitly counters what can be

[1379] Wachter, Mittelstadt and Floridi (2017).
[1380] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' [2017] 19.
[1381] Wachter, Mittelstadt and Floridi (2017) 39.
[1382] Ustaran and International Association of Privacy Professionals (2012) 139.
[1383] Mendoza and Bygrave (2017) 1.
[1384] Clifford and Ausloos (2017) 37.

referred to as the 'automation fallacy', i.e. the general assumption that automating or 'algorithmifying' decision-making renders such processes neutral, objective, and fair.[1385] Indeed, it is not difficult to notice that such an assumption is far from being correct in practice.[1386]

In spite of these high hopes, it has been argued that the provision is inoperable and blurred for a few reasons. First, the term 'solely automated', if read literally, is a narrow one. This creates the risk that some cases could slip through the cracks. For example, in behavioural marketing campaigns, data concerning personality traits and browsing habits of individuals is collected and automatically segmented into predetermined market segments. Assuming that the data collected is personal data, would the act of determining the qualities of each market segment be sufficient to mean that this is not a fully automated system?[1387] If solely automated decisions are only those in which there is no human involvement whatsoever, then this is a very high threshold. The Article 29 Working Party's view is more lenient. According to its recent opinion, *'to qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision.'*[1388] In section 9.2.3.2, it was noted that human decision-makers are prone to algorithmic biases as they often perceive AI to be more objective. Such human oversight is not sufficient to abandon the protection under Article 22 (1) of the GDPR. As the Article 29 Working Party suggests, what makes a difference is the authority to *challenge* the AI outcomes.

On the other hand, there is a risk that the Article 22 of the GDPR protection could extend too broadly and cover irrelevant cases. To illustrate, the decision of an ATM not to withdraw money is considered solely automated data processing. Some scholars believe that this should not be dealt with under Article 22, stating that it can be seen from the wording of the article that its objective is to protect a data subject from privacy-invasive processing applications that apply subjective criteria rather than intervene with established society-benefitting activities such as issuing a speeding ticket.[1389] Still, the line is difficult to draw. It is not impossible to conceive a situation in which receiving a ticket feels like being penalised with no human recourse, thus compromising human dignity. Ideally, the privacy invasiveness should be assessed in advance for each decision. A privacy impact assessment can be a good way to do so.[1390]

Only those automated decisions that produce legal effects concerning a data subject or affect her significantly are relevant for Article 22 of the GDPR. Recital 71 in the preamble to the GDPR mentions the refusal of 'online credit applications' and 'e-recruiting practices' as two examples of an automated decision with similarly significant effects. 'Similarly significant' could signal an intention that the consequences of a decision must have a non-trivial impact on the *status* of a person relative to other

[1385] Ibid.
[1386] Ibid. See also Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016).
[1387] Ibid.
[1388] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 10.
[1389] Mendoza and Bygrave (2017) 1.
[1390] Bygrave (2001) fn 42.

persons – just as legal effects typically do. Being placed in a different credit score category or not being offered a job certainly does have an impact on a person's status.[1391]

Could emotional impact be considered similarly significant? During the negotiations for the data protection directive in 1995, the EC took the view that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect those persons.[1392] However, this view was taken based on the text of the draft DPD that expressly required an *adverse* effect – a requirement that was later omitted from the enacted directive.[1393] The interpretation could change if the impact had a discriminatory dimension. For instance, in 2003, prof. Sweeney discovered that on ad trafficked websites, a black-identifying name like hers was 25% more likely to be shown an ad suggestive of an arrest record. If one could argue that she was significantly affected by pervasive racism as exemplified by the advert delivery, placing the ad could be prohibited under Article 22 of the GDPR.[1394] Seemingly, the Article 29 Working Party does not oppose this argument, although it notes that '*in many typical cases targeted advertising does not have significant effects on individuals.*'[1395] Commenting on the Article 29 Working Party's opinion, some scholars have expressed disagreement and warned that targeted advertising often relies on highly intrusive profiling, which in turn leads to serious violations of privacy and other rights.[1396]

Another issue at stake is the individual nature of the right. Returning to Sweeney's example, one could ask whether the discriminatory advertising influenced Sweeney herself or black people as a group.[1397] The Article 29 Working Party acknowledged that processing that might have little impact on individuals may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults.[1398] Moreover, the Article 29 Working Party did not rule out the possibility of a two-dimensional impact, incurring consequences for an individual and a group.[1399]

All in all, the right not to be subject to automated decision-making is a legal conundrum. Besides the perplexing language in the first paragraph, Article 22 of the GDPR contains three important carve-outs. The right – or better stated, the prohibition – does not apply when the processing is (a) necessary for

---

[1391] Ibid.
[1392] Commission, 'Amended proposal for a Council directive on protection of individuals with regards to processing of personal data and on the free movement of such data' [1992] COM(92) 422 final – SYN 287, 26–27.
[1393] Ibid.
[1394] Lilian Edwards and Michael Veale (2017) 7. To be precise, profiling that led to placing the ad would be prohibited.
[1395] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 10.
[1396] See for instance Kaltheuner and Bietti (2017) 16. Being manipulative and harmful, profiling for adversting purposes may affect many other rights of data subjects in addition to that of privacy. At this point, it is important to emphasize that both profiling for the purpose of targeted advertising and targeted adversting itself may be harmful. However, because profiling is instrumental to targeted adversting, disentangling is difficult.
[1397] Lilian Edwards and Michael Veale (2017) 7.
[1398] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 11.
[1399] Ibid.

entering into, or performance of, a contract; (b) authorised by EU or member state law;[1400] or (c) based on the data subject's explicit consent.[1401]

These three exceptions are only allowed as long as adequate safeguards have been put in place. If automated decision-making is authorised by law, then this law should also lay down safeguards for data subjects' rights and freedoms. As for the remaining two exceptions, a set of safeguards from Article 22(3) of the GDPR applies. These safeguards, which resemble the concept of a due process in public law, are introduced below.

9.3.3.3.2. The right to contest – technological due process?

In all three exceptional situations mentioned above, a data subject, apart from the general notification requirements and right of access in Articles 13-15 of the GDPR, may not know much about the decision-making process and its possible consequences.[1402] For example, solely automated decision-making cannot be avoided when entering into a contract with an insurance company, but is rarely disclosed.[1403] Even when the information is provided in advance, it can easily be buried under other information in the contract form. As a result, data controllers are allowed to exercise full discretion regarding whether automated decision-making is necessary for contractual obligations, while the data subject is unable to object to it.[1404] A similar situation occurs when data is processed on the basis of explicit consent. Consent, including explicit consent, suffers from 'desensitisation'. Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when asked to do so.[1405]

Because neither a contract nor explicit consent seems to guarantee sufficient protection, Article 22 of the GDPR provides extra safeguards: the right to contest the decision, the right to obtain human intervention, and the right to express one's point of view.

According to the Article 29 Working Party, obtaining human intervention is essential.[1406] Any review must be carried out by someone who has the appropriate authority and capability to change the decision.[1407] In this way, the burden to obtain the human intervention will eventually be borne by data controllers, who will have to ensure that they have sufficient resources to provide this sort of intervention. The right to human intervention is complemented by two further rights: the right to express one's point of view and the right to contest (Article 22, paragraph 3). These two rights resemble the adversarial procedure in administrative or criminal law, where the law ensures that the weaker

---

[1400] *... to which the controller is subject and which lays down adequate safeguards.*' Recital 71 of the GDPR mentions a few scenarios where such laws could be found – monitoring and preventing fraud and tax-evasion, ensuring the security and reliability of a service provided by the controller.

[1401] 'Explicit consent' is not defined in the GDPR. The Article 29 Working Party suggests that the consent must be specifically confirmed by an express statement rather than some other affirmative action. Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' 18.

[1402] Wachter, Mittelstadt and Russell (2018).

[1403] For the example see Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 18.

[1404] Ibid.

[1405] Bart Custers, Simone van der Hof and Bart Schermer, 'Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10 SCRIPTed.

[1406] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 16.

[1407] Ibid., 10.

party has the possibility to express himself and to challenge the opponent. The term 'contest' connotes more than 'object to' or 'oppose'; in other words, a right to contest is not simply a matter of being able to say 'stop', but is akin to a right to appeal.[1408] The right to appeal is an essential part of the due process in criminal and/or administrative legal procedures. Due process refers to a set of procedural safeguards intended to balance power and information asymmetries between the parties. Such asymmetries are also present in the relationship between data collectors and data subjects. Like governments, the dominating data collectors have the power to curtail users' freedom. Quasi due process rules, such as the right to contest, could thus be a good fit for the unique situation in the data economy.

If the appeal process is to be fair, it must carry a qualified obligation to provide the appellant with reasons for the decision.[1409] Thus, as a quasi appeal right, the right to contest should have such an informational dimension. One reference to it can be found in Recital 71 of the GDPR, which explicitly points to the right to explanation when it gives guidance in relation to Article 22(4)'s safeguards. There has been a lively scholarly discussion on the legal nature and the scope of this right to explanation.[1410] Some believe that an explanation could help in responding to automated decisions but is neither legally binding nor necessary.[1411] Others have argued, convincingly, that even though explanation was not mentioned in the binding text (or was even removed from it in the course of the GDPR negotiations), it should be extrapolated from the right to contest as its necessary pre-requisite.[1412] Indeed, if affected individuals lack the information that they need to effectively respond to a data controller's claims, resulting hearings will resemble a 'scene from Kafka.'[1413]

To be fair, the appeal process must also set certain obligations for the decision-maker, i.e. data controller. These obligations should include (at the very least) an obligation to hear and to consider the merits of the appeal.[1414] A contestation scheme has been suggested, consisting of the assessment of the scope of the data analysis, the accuracy of the data, the accuracy of the (analysis) calculation, and the interpretation of the (analysis) calculation that leads to a decision.[1415] The latter in particular is what makes data-driven decisions prone to challenges on the grounds of being unfair or unsubstantiated even when there exist no technical errors in the analysis or misrepresentation in the training data. To further extrapolate from administrative law, another duty imposed on the decision-maker is that of an independent 'judge'. The task of being an independent adjudicator could be taken on by a data protection officer, given that her independency is required by law.[1416]

As in the case of the right to object, the practical application of the right in Article 22 of the GDPR is a challenge. In an online environment, the Article 29 Working Party suggests the following form of the appeal process. At the point when an automated decision is delivered to a data subject, data controllers

---

[1408] Mendoza and Bygrave (2017) 16.
[1409] Ibid.
[1410] See for instance Wachter, Mittelstadt and Floridi (2017); Lilian Edwards and Michael Veale (2017); Goodman and Flaxman (2016).
[1411] Wachter, Mittelstadt and Floridi (2017).
[1412] Selbst and Powles (2017).
[1413] Danielle Keats Citron, 'Technological Due Process' 85 Washington University Law Review 1249.
[1414] Ibid.
[1415] Emre Bayamlıoğlu, 'Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation' (2018) 43 <https://ssrn.com/abstract=3097653> accessed 10 June 2017.
[1416] Article 38(3) and Recital 97 of the GDPR.

should provide a link to the appeal process with agreed time scales for the review and a named contact point for any queries.[1417] Mozilla has recently implemented an interesting self-regulatory version of a quasi appeal right. Its solution comes in effect *before* a decision is made. For instance, before Mozilla's AI system deletes a comment because of its toxicity, it allows the writer of the post to express her opinion and challenge the decision.[1418]

9.4. Provisions on profiling as control affording entitlements

9.4.1. Enablers to data subjects' control

The main conclusion that can be drawn from this chapter is that the GDPR's profiling-related provisions enhance control of data subjects over data in three different ways.

First, the GDPR explicitly allows the application of data protection law in profiling cases. Nowadays, profiling is embedded into the fabric of automated data processing in the data economy, manifesting in many ways, ranging from those with little impact on data subjects to those that may significantly infringe upon their fundamental rights. The three scenarios in section 9.2.1 showed that profiling may violate individual privacy, equality, and even democracy (by limiting electoral autonomy). The clear recognition of profiling under the GDPR is a first step towards a better handling of the profiling issues.

Second, the profiling-related provisions work as a choice architecture, helping users feel in control and nudging them towards decisions in their interest. This choice architecture is composed of three groups of rules relating to a) understandable and useful explanations, b) viable and easily accessible options to object, and c) possibilities to put limits to computability and 'algorithmic fallacy'.

Third, in Article 22 (4) of the GDPR, the choice architecture for data subjects is upgraded to the level of a quasi due process. While the choice architecture relates to the organisation of the context that benefits a data subject, the due process directly acknowledges the power imbalances in relation to data, which resemble relationships in administrative or even criminal processes.

9.4.2. Limits to data subjects' control

However, neither choice architecture nor due process escape the basic problem with individual rights under the GDPR: that is, the false assumption that individuals are indeed capable of asserting their right to access, rectify, erase, block, and object because they are aware that information about them is being processed and by whom.[1419] Individuals are prone to manipulation, uninterested in gaining extra information, and burdened with vast amounts of information.[1420] In addition, the due process

---

[1417] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 16.

[1418] A presentation of Andrew Losowsky on February 27, 2018, at the ISP tech talk event at Yale Law School, New Haven. This solution resembles the more established Online Dispute Resolutions (ODR) which are a form of alternative dispute resolutions and take advantage of the speed and convenience of the Internet and ICT. ODR is the best (and often the only) option for enhancing the redress of consumer grievances, strengthening their trust in the market, and promoting the sustainable growth of e-commerce. Hence, e-commerce has been the most natural field for the application of ODR. For instance, one well-known success story is eBay's implementation of online dispute resolution. Paolo Cortes, 'What should the ideal ODR system for e-commerce consumers look like? The Hidden World of Consumer ADR: Redress and Behaviour' (*CSLS Oxford*, 28 October 2011) <https://law.ox.ac.uk/sites/files/oxlaw/dr_pablo_cortes.pdf> accessed 14 June 2018.

[1419] Moerel and Prins (2016) 8-9.

[1420] Alessandro Acquisti, 'From the Economics of Privacy to the Economics of Big Data' (2014) 17-18 <https://www.heinz.cmu.edu/~acquisti/papers/economics-big-data-acquisti-lane-book.pdf> accessed 25 August 2018.

idea is worryingly underdeveloped and ambiguous, asking for judicial interpretation, which is not likely to occur in the near future. After all, Article 22 of the GDPR was also part of the EU data protection directive, but it never underwent a judicial revision.[1421] These drawbacks were noted by the Article 29 Working Party, which pointed to the necessity for controllers' intervention in such cases. Specifically, controllers should conduct frequent assessments on the data sets they process to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations.[1422] However, data controllers, and digital platforms specifically, have not been eager to accept these extra duties. On the contrary, they have tried, though not always successfully, to avoid their duties by claiming a neutral stance in relation to personal data processing.[1423] this problem has not gone unnoticed. In the recent years, regulators have started to more actively monitor and regulate platforms, in particular their automated decision-making practices (such as content moderation).[1424] Some of these initiatives could to some extent be a replacement for Article 22, or could at least offer some inspiration regarding what is feasible.

9.5. Conclusions

Chapter 9 sought to answer the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* This research sub-question refers to data subject rights as a whole but in this chapter it was narrowed down to the provisions of Article 21 and 22 of the GDPR. It was explored what these two provisions entail and in what ways they contribute to data subject control.

Section 9.2. provided the reader with the essential context on profiling as a building block of the data economy. Profiling is particularly useful as a technique to generate predictions by assuming that certain characteristics lead to certain behaviour. However, the knowledge that is derived from data with the help of profiling is no absolute truth and may negatively influence individuals. Two major risks are discrimination and invasions of privacy. Section 9.3. discussed how the GDPR tackles the risks of profiling – specifically the focus was on the right to object and the right not to be subject to automated decision-making.

Finally, in section 9.4. it was showed that GDPR's profiling-related provisions enhance control of data subjects over data in three different ways: as explicit recognition of profiling as personal data processing, as the building block of the choice-architecture for data subject, and as the facilitator of a quasi due process. However, the rights face the challenge of being under-applied due to the fact that individuals are prone to manipulation, uninterested in gaining extra information, and burdened with vast amounts of information.[1425]

[1421] Mendoza and Bygrave (2017).
[1422] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' 16.
[1423] C-131/12, *Google Spain* [2014] ECLI:EU:C:2014:317.
[1424] Commission, 'Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions; Tackling online disinformation: a European Approach' (2018) COM(2018) 236 final.
[1425] Alessandro Acquisti, 'From the Economics of Privacy to the Economics of Big Data' (2014) 17-18.

10. CONCLUSIONS AND RECOMMENDATIONS

10.1. Introduction

This chapter answers the key research question of this thesis: *Are the data subject rights under the EU law effective in the data-driven economy?*

To some extent, the key research question was addressed in Chapters 5-8, which investigated entitlements that data subjects enjoy under the data protection laws, implications that the data-driven economy has for them and whether these entitlements afford control to data subjects. These chapters already pointed out multiple examples of ineffectiveness of the current legal framework. To provide a complete answer to the key research question, it is necessary to assess effectiveness of the rights in a more structured manner and, depending on the outcome, recommend solutions. Chapter 10 takes on this task. By doing so, this chapter also answers the fifth research sub-question on possible solutions for ineffective data subject rights.

This chapter first summarises and substantiates the key findings of the thesis by introducing a benchmark comprising the data protection principles in Article 5 of the GDPR in section 10.2. These principles are (1) lawfulness, fairness, and transparency, (2) purpose limitation, (3) data and storage minimisation, (4) accuracy, integrity, and confidentiality, and (5) accountability. The principles represent the key goals of the EU data protection law and enshrine fundamental rights to privacy and data protection. If data subject rights are not able to materialise data protection principles, they are also not able to establish effective control. The effectiveness assessment substantiates what the previous chapters have already revealed: that data subjects' control rights are, to a large extent, flawed. The limits put on data subject rights by the new economy of continually reoptimising data-driven systems and complex internal surveillance functionalities are simply too severe.[1426]

Hence, without placing too much hope in the idea of individual control over data, the possibility of shifting attention to solutions outside the boundaries of data subject rights is considered in section 10.3. Previous chapters of this thesis indicated at many points that technology and legal mechanisms outside of data protection law can be useful to ensure control of individuals.[1427] These options, which are referred to as 'a holistic approach to control', are discussed in section 10.3. of this chapter.

10.2. (In)effectiveness of data subject rights

As was explained in Chapter 1, this study is based on the hypothesis that subject rights have the potential to enhance the individual position in the data-driven era. In the modern data economy, harm occurs due to controversial secondary data use rather than mere data collection. Data subject rights could work as use regulation and enable control that would extend beyond consent's take-it-or-leave-it approach.[1428] This assertion is supported by the facts that the section on control rights was expanded

[1426] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1.
[1427] See for instance Chapter 7 (section 7.6.1.), Chapter 6 (section 6.5.2.), Chapter 5 (section 5.3.3.).
[1428] Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press, 2016) 237.

in the updated EU data protection law and that the CJEU's recent interpretations strengthen the RTBF.[1429]

However, there is a gap between data subject rights when understood as law in the books and when applied in practice. As described in section 4.5., this ineffectiveness has technological, economic, and psychological causes, all of which are rooted in the specific characteristics of the data-driven economy. *Technological* causes refer to the intangible and invisible nature of data-driven software, which opens up possibilities to duplicate and share data in opaque and less controlled ways than physical goods. Control rights are mostly engaged in controlling the surface functionalities of the systems, whereas contemporary design practices emphasise modularity, continual rewriting and run-time upgrades, and seamless flow across platforms and applications.[1430] In such an environment, it becomes much more difficult to exercise effective control over data. *Psychological* determinants often prevent individuals from exercising effective control over data. Data subjects lack the ability and motivation to scrutinise key details of personal data processing necessary to make informed decisions about their data.[1431] Finally, *economic* determinants refer to the market forces that have created a situation in which data data controllers' dominance over digital information is no longer counter-balanced by control of other actors. Data reuse business models used by these controllers are opaque, technologically complex, and often cross the boundaries of data subjects' expectations.[1432]

10.2.1. The effectiveness assessment

To effectively control personal data, data subject rights must help an individual increase her awareness of and influence over data processing in a way that pursues certain values. Therefore, adequately protected values work as a benchmark for effective data subject rights. Chapter 2 identified four such values: autonomy, privacy, transparency and power asymmetry.

Fundamental values are open notions that are difficult to articulate. To simplify the effectiveness assessment, the data protection principles from Article 5 of the GDPR are used as a framework to answer the key question of this thesis. Content-wise, the Article 5 principles are very close to the four fundamental values (autonomy, privacy, transparency and power symmetry). They aim to establish boundaries to data processing and offer guidance to data controllers and processors to handle personal data in a legitimate and responsible way. These principles are (1) lawfulness, transparency of data processing and fairness[1433] (2) specification and limitation of the purpose,[1434] (3) data minimisation and storage limitation,[1435] (4) accuracy, integrity, and confidentiality of personal data,[1436] and (5) accountability.[1437]

[1429] See Chapter 7, section 7.4.1.
[1430] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1, 18.
[1431] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016, 19.
[1432] They also exceed regulatory expectations and supervisory powers. Pasquale (2015) 2.
[1433] Article 5, para. 1 (a).
[1434] Article 5, para. 1 (b).
[1435] Article 5, para. 1 (c), (e).
[1436] Article 5, para. 1 (d), (f).
[1437] Article 5, para. 2.

10.2.1.1. Data subject control rights as a vehicle of lawfulness, transparency and fairness,

10.2.1.1.1. Lawfulness

The first element in the assessment framework is a three-fold principle consisting of the concepts of lawfulness, fairness, and transparency. Of these three concepts, lawfulness is the most straightforward. It requires that any processing of data be based on a legally recognised ground such as consent, contract, or public interest.[1438]

All data subject rights pursue the principle of lawfulness, but the right to information stands out. The requirement to provide information about the legal basis for data processing compels controllers to clearly present their arguments (justification) for the use of data. Specifically, if legitimate interest is used as a basis for data processing, controllers are obliged to carefully balance their commercial interests with the fundamental rights and interests of data subjects, ensuring that they are not at risk.[1439] By doing so, the right decreases power asymmetries as it empowers a data subject with knowledge of the data processing. The stronger party (the data controller) is forced not only to disclose the legal basis, but also to present reasons that justify the decision to use a specific basis.[1440] Based on that knowledge, a data subject may later exercise his other data subject rights.[1441]

Using the right to information as a vehicle of lawfulness presents several challenges. First, legal bases may be presented to data subjects as a *carte blanche,* meaning that they are deliberately drafted in a way that covers a wide range of cases.[1442] To some extent, such generalisation is indispensable. The multiple, dynamic, and opaque personal data flows are difficult to follow. In addition, contemporary software design practices emphasise modularity, continuous rewriting, and run-time upgrades.[1443] Consider Facebook, which incorporates over 9 million apps, each of them operating in a slightly different context, e.g., research, advertising, and analytics.[1444] All these apps access and use Facebook users' data, but legal bases on which they rely are different. Providing specific information about each of them would put an extra burden on data subjects instead of helping them understand (and possibly challenge) controllers' reasons for data processing.

The second challenge is implementation. If the basis of data processing is consent, then the information is conveniently integrated into the consent request. This ensures that data subjects are at least momentarily in touch with the information. However, when the legal basis for data processing is not consent, it may be more difficult to identify the addressee of information. The general public is often addressed in such cases, but this means that the most relevant addressees may miss it.

As the processing moves forward, data subjects gain more possibilities to control the lawfulness of data. Specifically, they may take actions so that the use of data is no longer lawful. For data that was

---

[1438] Article 5(1)(a) of the GDPR.
[1439] Chapter 5, section 5.3.1.1.1.
[1440] Ibid.
[1441] Chapter 5, section 5.1.
[1442] Ibid.
[1443] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1, 18.
[1444] Brittany Darwell, 'Facebook platform supports more than 42 million pages and 9 million apps' *Adweek.com* (27 April 2012) <http://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/> accessed 22 may 2018.

collected on the basis of one's consent, withdrawal is always possible.[1445] If data is being processed on the basis of legitimate interest, a data subject has the option to object.[1446] If a data subject has consented to the use of her personal data to make automated decisions, she may challenge the processing by invoking her right to contest.[1447] In theory, these three types of control seem promising, but in practice they prove to be less effective. None of them can escape the basic problem with individual rights, that is the false assumption that individuals are indeed capable of asserting their right to access, rectify, erase, block, and object because they are aware that information about them is being processed and by whom.[1448] As mentioned in a previous chapter, individuals are prone to manipulation, uninterested in gaining extra knowledge, and burdened with vast amounts of information.[1449] In addition, the right to contest is worryingly underdeveloped and ambiguous, requiring judicial interpretation, which is not likely to occur in the near future. Thus, data subject rights are a weak vehicle of lawfulness. In the complex, dynamic, and opaque data-driven environments, control over lawfulness mostly remains the exclusive task of data controllers.

10.2.1.1.2. Transparency

Transparency of data processing is one of the key data protection principles, intended to help strike a balance of powers between the data controller and data subjects. More transparency should translate to more control for data subjects.[1450] To be a vehicle of transparency in the data-driven economy, data subject rights should specifically target the following two aspects of transparency: transparency of data flows and transparency of data use.

Regarding *data flows*, one important mechanism to boost transparency and control is the right to information about data sources and recipients. When a data subject is aware of the flow of his data, he may decide not to share data in the first place. However, providing information about every recipient and source may be a challenging task for data controllers. As mentioned above, Facebook recently revealed that it cooperates with millions of third-party apps.[1451] Moreover, even though Facebook would in theory be able to disclose information about all potential data destinations, such information overload would hardly be of any use to data subjects.[1452]

The information about sources and recipients of data is not only useful at the moment when data processing starts: due to continuous system updates and flows of data, it is in fact more useful to have this information *ex post*. Under the access right, a data subject may inquire about sources and recipients of a specific dataset.[1453] While this may be a good approach for a data subject, it places a heavy burden on data controllers. To follow the data provenance (lineage), i.e., determine for each

[1445] Article 7 of the GDPR.
[1446] Article 21 of the GDPR.
[1447] Article 22 of the GDPR.
[1448] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016).
[1449] Alessandro Acquisti, 'From the Economics of Privacy to the Economics of Big Data' (2014) 17.
[1450] See for instance Chapter 5, section 5.2.
[1451] *Supra* n 1444.
[1452] Chapter 5, section 5.3.2.
[1453] Chapter 6, section 6.2.1.

data point where it came from and where it is going, the controller has to put a tag onto each data point. Means of doing this effectively, such as block chain, are still being developed.[1454]

Transparency of *data use* relates to transparency of AI techniques when applied to personal data. These have been further developed in recent years and have also become widespread.[1455] Both the right to information and the right of access ensure information about AI, but explaining its functioning and possible impacts is complicated. To provide complete and up-to-date information, controllers should carry out frequent assessments on the data sets they process and check for any bias or discriminatory elements.[1456] Viable ways to convey the information are being developed. In addition, algorithms may use aggregated personal data that cannot be attributed to a specific human being. In such cases, data control rights are inapplicable, but anonymised data may still lead to profiling and surveillance.[1457]

In contrast to the rights to information and access, the right to data portability focuses on sharing of data.[1458] However, data portability could also enable searches within the data that organisations hold about individuals.[1459] For instance, data could be ported to data analytics services which would provide deeper insights into the data. Thus, the right to data portability could enable greater literacy and transparency around how data is being used.[1460] The drawback of the right to data portability as a vehicle of transparency is that its scope is highly limited. The so-called inferred information that plays a pivotal role in understanding the functioning of the data economy, i.e. statistics and insights in behavioural patterns, falls outside the scope of the right.

Data subject rights could in theory be a vehicle of transparency. In fact, some have suggested that in the data-driven economy, the right of access has the potential to grant data subjects control over data processing.[1461] However, it has been demonstrated that user experience with that right is often negative.[1462] Furthermore, it appears that precisely the information in which a data subject has the most interest is often not available to her.[1463]

To achieve user control transparency alone is not sufficient and more than mere disclosure is needed. In particular, disclosure should be complemented with documentation of data lineage, monitoring of algorithmic biases, and a user-friendly access interface. However, these aspects probably go beyond

---

[1454] However, block chain itself raises some data protection related issues, among others it may prevent data subjects from erasing their peronal data. For more details see Finck (2018).
[1455] Chapter 9, section 9.2.
[1456] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017). Also see Global Future Council on Human Rights 2016-2018 (World Economic Forum), 'How to Prevent Discriminatory Outcomes in Machine Learning' (2018) 23.
[1457] Elena Esposito, 'Algorithmic Memory and the Right to Be Forgotten on the Web' (2017) 4 Big Data & Society.
[1458] Chapter 8, section 8.5.1.
[1459] Jenni Tennison, 'Data Portability' (2017) <http://www.jenitennison.com/2017/12/26/data-portability.html>.
[1460] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2016).
[1461] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2018) 7 International Data Privacy Law 233, 241.
[1462] Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 26.
[1463] Namely what is done with her data and why. Ibid., 26. Also see Chapter 6, section 6.4.

the GDPR provisions on data subject rights, as they would require data controllers' substantial input, the use of technological solutions, and lenient interpretation of legal provisions.

10.2.1.1.3. Fairness

Data processing must be done *fairly,* but the GDPR does not define what fairness means. Chapter 5 proposed two criteria to assess fairness: 'good faith' of the data controller and 'significant imbalance' between the controller and the data subject.[1464] Both criteria indicate that fairness should be assessed with particular consideration for the needs of an individual.

To be a vehicle of fairness, data subject rights should contribute to equality and honesty in relationships between controllers and data subjects. Under the framework of the right to information, certain information should be communicated to a data subject only if this is necessary for the reason of fairness.[1465] Two examples are information about automated decision-making and information about data storage. Today, data is often processed with minimal human interaction, which increases the risk of unfair outcomes.[1466] Likewise, the information on storage is critical, as storage is increasingly cloud-based. Thus, in a data-driven economy, both pieces of information should be provided to a data subject at the point of data collection. If any relevant updates or changes occur later in time, they should be communicated to a data subject too. However, this approach has drawbacks: privacy policies may become longer, more complex, and almost pervasive. Loading data subjects with additional information may in turn lead to unfair processing.

Article 22 of the GDPR specifically aims to infuse fairness into automated decision-making processes by limiting those data-driven decisions that may have consequences for data subjects but are not monitored by humans.[1467] Prohibiting solely automated decisions would be the easiest way to establish a balance. However, given that AI also has many positive uses, this is not a recommendable strategy. Therefore, Article 22 strikes a balance by imposing a prohibition only on those AI-driven decisions that may have serious, far-reaching impacts on individuals. By doing so, the article also pursues the principle of proportionality, which some see as an important component of fairness.[1468]

From the data subject's point of view, the so-called contesting scheme in Article 22(3) is particularly relevant. The scheme consists of two rights, the right to receive an explanation of automated decisions and the right to challenge those decisions, and represents one more attempt to increase fairness in data processing.[1469] However, all the rights under Article 22 of the GDPR are considerably limited due to the narrow definition of solely automated decisions and the difficulties of setting up an explanatory and contesting process in practice.[1470]

The right to object and the righ to erasure (RTBF) pursue fairness by allowing data subjects to block data controllers from certain types of data processing. The right to object empowers data subjects to *ex post* challenge legitimacy of an *ex ante* balancing test through which a controller justified data

---

[1464] Chapter 5, section 5.2.
[1465] See for instance Chapter 5, section 5.3.1.2.1.
[1466] Among others, power imbalance and violations of the principle of good faith. See page 4 above.
[1467] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness Data Protection and the Role of Fairness' (2017) CiTiP Working Paper Series, 37. See also Chapter 9, section 9.3.3.3.
[1468] Ibid., 39.
[1469] Chapter 9, section 9.3.3.3.1.
[1470] See section 9.3.3.3.2. for some early ideas.

collection.[1471] By invoking the right to erasure, data subjects may remove the data that they voluntarily shared with data controllers in the past.

Data subjects' ability to have data deleted is contingent with their awareness of (undesirable) data processing. As data processing, in particular profiling, is often opaque, it is difficult to note when certain data processing is problematic and objectionable. Data-driven software used for profiling typically draws on aggregated personal data that cannot be attributed to a specific human being. Although such data is still relevant for the profiling and surveillance of citizens, it may be inaccessible to the delisting in accordance with the RTBF.[1472] In addition, such inferred data is composed of characteristics assigned to a person based on his online behaviour in comparison to a large group of (similar) users. This type of data is at the heart of data-driven algorithms, as it enables predictions, which companies need for various commercial purposes. If a single data subject requests erasure, it is unlikely that this will make much difference for a trained model and/or the algorithmic outcome.[1473] To make effective use of the RTBF to alter models, whole groups would need to collaborate explicitly or implicitly to request erasure, which is highly unlikely.[1474] Furthermore, the nature of global data (flows) challenges the right to deletion. After a successful delisting request to Google, researchers were still able to identify 30-40% of the deleted URLs.[1475] This suggests that removal of search results falls short of digital 'forgetting'. Moreover, delisting is only effective on European servers, since Google rejected EU demands for a worldwide application of the RTBF.

Data subjects' ability to object to data processing is contingent on a data controllers' willingness to create a digital environment that enables meaningful objection. Here, the risk is that controllers could manipulate the architecture of their systems and construct it in a way that satisfies formal requirements, but does little for data subjects' control.[1476]

To conclude, data subject rights are a weak vehicle of fairness for two reasons. First, the reality of the data-driven economy simply does not allow for a level playing field. Second, the characteristics of this economy permit or even encourage dishonest and controversial data practices which cannot be addressed by the mechanisms of data subject control.

10.2.1.2. Data subject rights as a vehicle of purpose limitation

The principle of purpose limitation requires that the purposes for which personal data is collected be specified and that the data only be used for these purposes.[1477] Any secondary data use, unless stipulated at the moment of data collection, is prohibited in principle. In the data-driven economy,

[1471] I.e., the balancing that happens at the initial data collection when possible legal basis are assessed. Clifford and Ausloos (2017).
[1472] Elena Esposito, 'Algorithmic Memory and the Right to Be Forgotten on the Web' (2017) 4 Big Data & Society.
[1473] Regardless of all the difficulties, results of algorithmic analyses should reflect individuals' real characteristics and should therefore be adjusted dynamically to their 'personas'. In this vein also see Julie E Cohen, 'What Privacy Is for' (2012) 126 Harvard Law Review.
[1474] 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 Duke Law and Technology Review, 36.
[1475] Minhui Xue and others, 'The Right to Be Forgotten in the Media: A Data-Driven Study' (2016) 4 Proceedings on Privacy Enhancing Technologies.
[1476] For details see Chapter 9, section 9.4.
[1477] Article 6(b) of the DPD.

reuse of data is the key business model, and frequent changes of purposes are inherent to it. Thus, by default, the data-driven economy challenges the idea of purpose limitation.

Control rights address this issue to some extent. The right to information includes a provision that any change of the purpose of data processing must be communicated to data subjects. However, such updates are often general and easily missed (e.g., an online privacy policy update). In addition, an update is no longer needed after data has flown to a third party. In such cases, data subjects may turn to the secondary data controllers with an access request,[1478] but due to the scale of data sharing this is time-consuming and requires disproportionate efforts.[1479]

The right to erasure emphasises the principle of purpose limitation by allowing data subjects to prevent those uses that fall short of being relevant for the primary data purpose (and which, most likely, do not meet users' privacy expectations).[1480] However, in an increasingly personalised Internet, almost every bit of personal data can be argued to be relevant.[1481] To allow unforeseen future uses, data processing is often based on either open or extremely detailed descriptions of purposes of data processing. As a result, any secondary use can be interpreted as relevant in relation to the purposes for which the data was collected.[1482] Although such unspecified or unlimited purposes are not allowed under the GDPR, they are widespread.[1483] This makes it more difficult for the RTBF to tackle irrelevant data processing. Furthermore, purpose limitation does not apply when controllers use data on an aggregated level. Anonymised data falls outside the scope of data protection law.[1484] Data controllers are free to reuse, monetise, or otherwise exploit non-identifiable datasets. Although such data processing may still have an impact on a data subject (as a member of a group), data subject rights cannot be exercised in these situations.

The principle of purpose limitation could be one of the most powerful control mechanisms for data subjects. However, due to its unrealistically broad scope and its inherent tension with business objectives, it often fails to deliver – either alone or as a component of data subject rights.

10.2.1.3. Data subject rights as a vehicle of data minimisation and storage limitation

The principles of data minimisation and storage limitation enhance all other data protection principles analysed above. Limiting storage time and the amount of data decreases the risk of wrongful or extensive uses, as less data is exposed to potential abuses for a shorter time period. This principle correlates with the principle of proportionality, which not only represents a general, guiding principle for data protection law,[1485] but also imposes a specific requirement that data processing is adequate,

---

[1478] Information Commissioner Office, 'Subject access request' <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/> accessed 22 May 2018.
[1479] Chapter 6, section 6.2.2.2.
[1480] Chapter 7, section 7.4.2.1.1.
[1481] Graux H., Jeff Ausloos and Valcke Penny, 'The Right to Be Forgotten in the Internet Era' in J Pérez, E Badía and R Sáinz Peña (eds), *The Debate on Privacy and Security over the Network: Regulation and Markets* (Ariel 2012) 103. See also Zarsky (2018).
[1482] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice' (2011) 8 SCRIPTed 229, 244.
[1483] Willem Debeuckelaere v Facebook Ireland Ltd., Facebook Inc. and Facebook Belgium Bvba., Dutch-language Brussels Court of First Instance, judgement from 16 February 2016, p. 59 <https://pagefair.com/wp-content/uploads/2018/04/Belgian-Court-judgement.pdf> accessed 22 May 2018.
[1484] Chapter 7, section 7.4.2.1.1.
[1485] See Recital 4 of the GDPR.

relevant, and not excessive. In the GDPR, proportionality plays the role of a guiding principle in cases when personal data processing creates a conflict of legal rights.[1486]

The information on limitation of storage and amount of data in privacy policies gives users an assurance that the company will not sell their data to advertisers or other third parties.[1487] However, policies often provide a long list of exceptions, e.g., extended storage to share data with the government. In addition, companies often anonymise data to fulfil the obligations under the principle. Anonymised data can be used and stored in an unlimited amount, and although such datasets are not linked directly to an individual, they may lead to negative societal impacts such as discrimination of underrepresented groups of people.[1488]

The most direct *ex post* mechanism of control over stored data is the right to erasure. However, this right comes with some limitations too. First of all, although the GDPR stipulates that deletion happens without undue delay, technically this process is not immediate. For example, Facebook warns that it may take up to 90 days to delete data stored in its backup systems.[1489] Second, some data is stored outside of the deleted Facebook account. For example, a user's friend may have copied their conversations on Facebook Messenger to her phone or laptop. The deletion has no effect on such data processing. Finally, copies of some materials (for example, log records) may remain in Facebook's database. Although they are dissociated from personal identifiers (i.e., anonymised), the risk of de-anonymisation is never completely eliminated.

10.2.1.4. Data subject rights as a vehicle of accuracy, integrity, and confidentiality

Control rights that can be exercised in the course of data processing are of special importance for pursuing the principles of accuracy, integrity, and confidentiality. First, the right of access may be used to check whether personal data that a data controller holds is still accurate.[1490] Second, the right to erasure (RTBF) may help in cases in which inaccuracy is detected – such data can be deleted on the basis of no longer being accurate (i.e., lawfully processed).[1491] In some limited cases, the right to contest automated decision-making under Article 22 of the GDPR may enable control over accuracy of the data and (algorithmic) analysis.[1492]

However, to completely control the integrity and confidentiality of data, a data subject would need to engage in assessing risks of loss, unauthorised access, destruction, etc. of personal data. This seems impossible in the context of the data-driven economy because it would require checking all cases of data sharing, third-party apps' uses, and some highly technical aspects of data management. The scalability and technical complexity of data processing prevent data subject rights from being a meaningful vehicle of accuracy, integrity, and confidentiality.

[1486] Els J Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013), 419.
[1487] Dropbox's privacy policy <https://www.dropbox.com/privacy> accessed 22 May 2018.
[1488] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy and Technology, n. 9.
[1489] Facebook's help centre <https://www.facebook.com/help/359046244166395/> accessed 22 May 2018.
[1490] Chapter 6, section 6.1.
[1491] Chapter 7, section 7.4.2.1.1.
[1492] Emre Bayamlıoğlu, 'Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation' (2018) <https://ssrn.com/abstract=3097653> accessed 22 May 2018.

In the discussion on data portability, it was suggested that the right could be used to send data to a third party to conduct an impartial check of accuracy, integrity, and confidentiality of data.[1493] However, this is further proof that data subjects alone are not able to control accuracy and integrity, and that external support is indispensable. In addition, the idea faces an important limitation: the narrow definition of the right. Portability only applies to data provided by a data subject. The profiled and other inferred data falls outside the scope of the right to data portability.

10.2.1.5. Data subject rights as a vehicle of accountability

The principle of accountability requires controllers to be responsible for their compliance with the GDPR's principles and to be able to demonstrate that.[1494] For example, controllers may have to adopt 'data protection by design' measures (e.g. pseudonymisation techniques), run staff training programmes, conduct privacy impact assessments,[1495] or hire (a) data protection officer(s).[1496]

Although accountability is one of the most influential concepts on the duty side of data protection law, it is relevant for the control side dominated by data subject rights as well.[1497] In fact, data subject rights may often function as vehicles of accountability. For example, in an attempt to limit the negative impacts of automated decision-making, the GDPR uses the section on data subject rights to set some key limitations. Data subjects must be informed about the way in which automated decisions are made and about possible consequences. This means that data controllers must make clear how their algorithms are used, and must determine in advance what negative consequences data subjects may expect (e.g., seeing irrelevant or even upsetting fake news). Furthermore, under Article 22 data subjects may contest automated decisions. This may create an extra layer of accountability because data controllers are forced to provide an explanation of and reasons for the use of AI.[1498] However, what looks promising on paper does not necessarily deliver in practice. The truth is that, in general, control rights fail to work as a vehicle of accountability. Because of the nature of data and the architecture of the data economy, data subjects have highly limited options to police data controllers. Moreover, control rights may be in conflict with accountability measures. For instance, data deletion is a building block of 'privacy by design' but it may impose restrictions on the right of access.[1499]

10.2.2. Concluding remarks

This section provided an answer to the first part of the key research question: *Are the data subject rights under the EU law effective in the data-driven economy?*

As was explained above, the answer is a clear-cut 'no'. Although the law in books appears promising, it fails in action. As it is utopian to expect that the developments in the data economy will soon cease, alternative solutions for individual control should be sought. This is exactly what the fifth research sub-

---

[1493] Chapter 8, section 8.6.1.2.
[1494] Article 5(2) of the GDPR.
[1495] A PIA is is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. It is advisable for all data processing, but required in the cases where fundamental rights are at a greater risk. See Article 35 of the GDPR.
[1496] DPO is is an appointed individual who advises implications of Data Protection law and develops the company's privacy and data protection policies. See Article 37 of the GDPR.
[1497] See Chapter 3, section 3.3.2.1., for the distinction between the duty- and the control-side of the GDPR.
[1498] Chapter 9, section 9.3.3.3.2.
[1499] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) forthcoming in International Data Privacy Law.

question tries to address: If data subject rights are not effective, are there any solutions to overcome their shortcomings? The following section provides an answer.

10.3. The way forward for data subject rights

10.3.1. Abandoning control rights

Given the ineffectiveness of control rights, one could easily argue that data protection law should focus more on the duties of data controllers and that the control side of it is redundant as it does little to improve the protection of personal data and overall legitimacy of data processing. In fact, Cohen has suggested that in light of big data, the paradigm of privacy as individual control should be abandoned: '*privacy's most enduring institutional failure modes flow from its insistence on placing the individual and individualized control at the center.'*[1500]

Abandoning data subject rights could be desirable not just because individual control over big data processing is a utopian goal, but also because it can be a hurdle to the safe and beneficial use of data. For instance, in genomics research, excessive data subject control can be an obstacle to innovation and science prosperity.[1501]

The GDPR does acknowledge, to some extent, the difficulty of exercising control. What is surprising is how the regulator dealt with the problem: instead of accepting that shortcomings are inherent to data subject control, the regulator reinforced data subjects' control rights. Specifically, this is seen in the fact that the GDPR comes with an extended and detailed list of data subject rights.[1502]

The rationale of the regulator's move may be the following: although control rights are ineffective or at least much less effective than we want them to be, they must remain part of data protection law because they do not only serve the objective of control but have other objectives too. First, data control rights can work as a 'social monitoring mechanism'. Consider the right to information: although data subjects in general disregard the information in privacy policies, this information may be useful to privacy advocates and journalists who are able to put pressure on companies in a different yet successful way. Second, control rights can be a 'self-defence mechanism' as they are closely tied to enforcement mechanisms. A data subject may use her data subject rights to gather more information that could support her case against a data controller. In addition, when data subject rights are violated, this can be a trigger to complain to a data protection authority or to bring action to a court of justice. Third, control has symbolic meaning, as it reflects some pivotal values such as autonomy, privacy, and dignity. The mere fact that control rights are in place means that data subjects maintain their autonomy. Finally, control rights seem regulation 'light': they are cost-effective and easy to agree upon. Although they may be of little use for data subjects, they certainly give data controllers an extra nudge to more carefully consider data subjects' needs and rights.

Thus, what needs to be abandoned is not data subject rights, but the belief that they can be used to impose effective control over data flows. A shift in the vocabulary used to describe data subject rights

---

[1500] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1.
[1501] Effy Vayena and Urs Gasser, 'Between Openness and Privacy in Genomics' (2016) 13 PLoS Medicine 1,2. Also see: Moerel (2014) 55 (suggesting to abandon the right to object). It should be kept in mind that the GDPR solves this issue to some extent by introducing derogations in Article 23 and the regime for scientific research data processing in Article 89.
[1502] As well as from the political documents preceding GDPR. See Chapter 4, section 4.4.1.

could be helpful in this regard. That vocabulary should be adapted to their limited reach and effectiveness. Instead of users' control rights, they should be referred to as users' monitoring or self-defence rights. This would manage expectations with regard to their effects but would not completely water down their role within the data protection law.

In addressing the failure of data subject rights as a mechanism of individual control over data flows, a useful approach would be to look for alternatives. After all, if control rights under the GDPR are not effective, this does not mean that control as such is not desirable. As explained above, control remains an important normative objective, but the means to achieve it may differ.

10.3.2. Alternatives to data subject rights

The following sections explore (self-)regulatory approaches that may also enhance individual control over personal data. These approaches rely on (1) technological solutions and (2) legal provisions both inside and outside the domain of data protection law, save for the provisions on data subject rights. One may note that no economic alternative is proposed at this point. Although it is not difficult to agree that a major change in the business model of data-driven companies would probably be the best remedy for diluted individual control, I do not explore it as an option. The context of the data-driven economy is taken as a given in this thesis, which makes it the only setting in which inefficiencies of data subject rights are explored.

This section builds on the ideas expressed in previous chapters. However, below they are further synthesised and structured to provide a complete framework for an alternative, holistic approach to data subject control.

10.3.2.1. Turning to technological solutions

In his book *Code*, Lawrence Lessig emphasises the importance of a technical code in regulating the cyberspace by assigning it the same significance as to a legal code.[1503] Just like statutes, constitutions, or any other laws, the design of computer code may embed and protect certain values.[1504] In relation to automated processing of personal data, technology may promote values such as privacy, fairness, and control.[1505] The paragraphs below discuss technological design that embeds the concept of individual control and thus represents one possible alternative to traditional application of data subject rights.

The analysis of data subject rights in this thesis already indicated that in many cases, the use of technology (design) proves successful in helping individuals exercise control over data. Concerning the right to information, technology can be deployed to improve data subjects' cognition abilities. Swiss researchers have developed an AI tool that summarises key aspects of privacy policies.[1506] In this way, a data subject is provided with a concise overview of a company's data practices. A similar solution is

---

[1503] Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006) 114.

[1504] Hartzog carries over the same idea by arguing that the design of software and hardware is key in regulating data-driven environments. Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (2018).

[1505] In fact, the concept of 'privacy by design', which requires involving various technological and organisational components to implement privacy and data protection principles in systems and service, is a binding rule under the GDPR (Article 25). European Union Agency for Network and Information Security, 'Privacy and Data Protection by Design – from Policy to Engineering' (2014) 3.

[1506] Andy Greenberg, 'Polisis AI reads privacy policies so you don't have to' (*Wired*, 9 February 2018) <https://wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/> accessed 22 may 2018.

the visualisation of data policies through an online platform that allows for a 3-D illustration of data flows.[1507] In relation to the right of access, technical solutions are best implemented in the design of a service. If the right is implemented in a way that is easily accessible and user-friendly, e.g. offering a simple and open interface, more individuals could decide to exercise that right.[1508] Some recent yet immature solutions to guarantee access have been linked to developments in the areas of blockchain[1509] and AI technology.[1510] The right to objection under the GDPR explicitly foresees that data subjects should be able to exercise their right by automated means using technical specifications. One feasible way to implement the right to object is to integrate it with data processing. In the context of social networks, this would work in a similar way as the 'I don't like this ad' function enabled by social media providers for each ad that has been placed on the timeline.[1511] Data subjects could point to the ad that they found privacy-intruding and remove it instantly. Another option would be to implement the right as a privacy tool into a dashboard; this may not be as obvious, but it seems less annoying.[1512] Furthermore, various technical solutions have been suggested to implement the right to erasure (RTBF). For instance, expiration dates or some other forms of deletion-by-default could lead to effective deletion. The data subject would not be the one triggering the right, but the software itself would ensure the information was deleted after some time. In fact, this sort of erasure has recently been announced by Gmail, which will soon offer users an option to set up expiration dates for their emails.[1513] Finally, technology may help integrate all data subject rights into a 'privacy dashboard', an interface providing users with access to information on personal data and the configuration of privacy settings.[1514] A prime example of such a dashboard is *My data,* a movement launched by the Finnish government.[1515] The initiative seeks to give individuals practical means to access, obtain, but also use datasets containing their personal information from different sources, including traffic data, telecommunications data, medical records, financial information, and data derived from various online services.[1516]

In a commercial environment, technical implementations of the rights are often at the mercy of data controllers. This puts them at risk of falling short of the legal guarantees. Consider the right of access: people may feel falsely empowered by the opportunity to monitor a fragment of their online data, while the only way to obtain a whole picture would be to follow their digital traces in the background – a mission that goes beyond the abilities of a regular consumer. Using new technologies to facilitate individual control may also backfire. Blockchain strengthens the right of access by ensuring data subjects have access to a complete chain of transactions, but it is, at least in its public version, a barrier

---

[1507] Chapter 5, section 5.3.3.1.1.

[1508] However, the danger that such (typically commercial) implementation may be too restrictive remains present.

[1509] Before blockchain is actually used as a medium to make requests, it is of utmost importance that possible negative consequences for individual privacy are carefully assessed before blockchain becomes operable. One such solution could be the use of a private blockchain. See Finck (2017).

[1510] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016) 67.

[1511] As implemented by Twitter to address the problem of hate speech.

[1512] As implemented by Facebook.

[1513] Rachel Kraus, 'Here's how the new expiring Gmail's 'expiring feature' works' *Mashable (*27 April 2018) <https://mashable.com/2018/04/27/new-gmail-expiring-emails-confidential-mode/#BIkch1.15ZqO> accessed 22 May 2018.

[1514] Irion and others.

[1515] Antti Poikola, Kai Kuikkaniemi and Harri Honko, 'MyData – A Nordic Model for Human-Centered Personal Data Management and Processing' <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y> accessed 1 November 2017.

[1516] A similar UK initiative, which has winded down in the recent months, is the 'midata' project; <https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment> accessed 26 January 2018.

to the RTBF.[1517] A similar situation may occur in relation to the RTBF solutions: Gmail promises to enable expiration of emails but in fact only a link that replaces the email body expires. After an email has been deleted, there may still be a record of users sending and receiving self-destructing emails.[1518]

10.3.2.2. Legal solutions

The previous section demonstrated that technological solutions are one possible alternative to data subject control. The section below explores some legal solutions. This thesis has already indicated, at a few points, that provisions regulating data subject rights should not be isolated from the surrounding legal environment. The suggestion is to apply them holistically: that is, in combination with mechanisms from both inside and outside the domain of data protection law. In the following, some of these alternatives are described in more detail. First, a holistic approach to the GDPR is introduced. This approach acknowledges the complimentary nature of the GDPR's provisions addressed to data controllers and the control provisions addressed to data subjects. Second, holistic legal approach is presented. This approach takes advantage of legal instruments and regulatory strategies in domains other than data protection law. The reason to use them is simple: they could work as a substitute for data subject control rights, an invigorator of the rights, or both.

10.3.2.2.1. Holistic approach within the GDPR

Earlier in this thesis, some criticism of the GDPR's approach to data subject rights was expressed. It was argued that the provisions appear strong on paper whereas in practice they do not meet expectations.

Mantelero shares the opinion that control rights are becoming obsolete in the big data economy.[1519] As a solution, he proposes a system where control would not stem from individuals but, instead, from other actors in the economy, such as data controllers and data protection authorities.[1520]

Under the GDPR, Mantelero's vision is achievable. The GDPR imposes new, more extensive duties on data controllers. Shifting control to the protection side of data protection law does not necessarily mean that data subject rights are redundant.[1521] Yet the shift stresses the need to reconsider their relationship with controllers' duties. Data subject rights should not be seen as isolated, but should be complemented with the mechanisms from the duty side of data protection law. Specifically, actions of neutral third parties and data protection authorities could empower data subjects even when data subjects are less actively involved.[1522] Article 25 offers a prime example: according to this rule, controllers are required to *ex ante* ensure privacy-friendly design of their systems. This may be crucial

---

[1517] Michéle Finck, 'Blockchains and Data Protection in the European Union' (2017) Max Planck Institute for Innovation and Competition Research Paper 18/1.

[1518] '*… Google don't simply delete themselves like you'd expect. Instead, Gmail sends the recipient a dummy email with a hyperlink to the actual self-expiring message, which is what actually disappears when time expires. That means there will still be a record of users sending and receiving self-destructing emails, but not necessarily any info on what was contained in the message*.' 'Sam Rutherford, There Might Be a New Self-Destructing Message Feature in the Gmail Revamp' *Gizmodo* (13 April 2018) <https://gizmodo.com/there-might-be-a-new-self-destructing-message-feature-i-1825242833> accessed 22 may 2018.

[1519] Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking The "notice and Consent" paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law and Security Review 657.

[1520] Ibid.

[1521] See several reasons in section 10.3.1.

[1522] The idea of third parties' involvement in protection of personal data is also expressed in in relation to age verification and verification of parental consent in case of high-risk processing. See Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) 26.

for a data subject when she later exercises her right to erase or object. For instance, how quickly and thoroughly the right to erase may be invoked depends, to a large extent, on the initial design of the systems.[1523] Similarly, under Article 35, a controller is required to conduct a data privacy impact assessment whenever data processing includes automated decisions that have legal or otherwise significant impacts. The rationale is to prevent any harmful effects that these decisions may have due to inaccurate or illegitimate use of data. Although data subjects have some limited possibilities to challenge automated decisions under Article 22, these are only complementary to the regular checks by data controllers.[1524]

10.3.2.2.2. Holistic approach outside the GDPR

Not all the drawbacks of the big data economy can be resolved by strengthening data protection law. For instance, if data is anonymised and decisions are taken at a group level, neither control rights nor protection duties will mitigate the risk of negative societal impacts. Therefore, solutions must also be sought in legal domains outside data protection law. The sections below discuss four domains that are, in my opinion, most likely to mitigate the issue of diluted individual control in the data-driven economy. The list is not exhaustive, and many other relevant provisions could certainly be identified. For instance, some have indicated that solutions could be found in anti-discrimination[1525] or property law.[1526] Both ideas are compelling. However, anti-discrimination law draws on fundamental principles that are open by their nature and cannot be easily translated into tangible legal mechanisms.[1527] Furthermore, the idea of property law as a basis of data subject control may well fit the US legal system, but is less suitable to the EU views on data protection. For these reasons, these ideas are not explored in further detail. In any case, the aim of this section is not to provide a complete list but to introduce the holistic approach as one possible way forward.

10.3.2.2.2.1. Consumer protection

Applying consumer protection regulation to enhance data protection could importantly contribute to the mission of data subject rights. In particular, it could help them be a vehicle of fairness and transparency. Consider this example. In the data-driven economy, personal data is being used not only to provide a service but also to extract extra commercial value from that data. Doing so without telling the consumer could constitute an unfair commercial practice under 5(2) of the directive concerning unfair business-to-consumer commercial practices in the internal market.[1528] Thus, the unfair commercial practices directive could be used to mitigate negative impacts on individuals who, in the data-driven economy, play the dual role of consumer and data subject. The EU directive on unfair terms could work towards the same aim. The directive defines as unfair a term that, contrary to the requirement of good faith, causes a significant imbalance in the parties' rights and obligations arising

[1523] Simone Van Der Hof and Eva Lievens, 'The Importance of Privacy by Design and Strengthening Protection of Children ' S Personal' (2018) 23 Communications Law, 11.
[1524] Ideally DPIAs and PbD would be carried out simultaneously.
[1525] Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information and Communications Technology Law 74.
[1526] Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25 Computer Law & Security Review 507.
[1527] See also section 3.2.3. for more details.
[1528] Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' <https://www.ivir.nl/publicaties/download/1747.pdf> accessed 23 May 2018, 10.

under the contract, to the detriment of the consumer.[1529] Another detail is also important: consumer protection authorities may be quicker in reacting and may have better resources than data protection authorities do. In some recent cases that related to improper use of data, consumer protection, *and not* data protection, authorities were the first to initiate an investigation.[1530]

There is one problem with applying consumer protection law in a data-driven environment. In principle, consumer protection law applies to contracts that are based on monetary exchange.[1531] However, most of the data-driven services use a freemium pricing strategy, which is not based on money but on personal data exchange and thus may fall outside the scope of consumer protection law. Arguably, there will soon be more clarity on that. The EC's proposal for a directive on certain aspects concerning contracts for the supply of digital content has acknowledged these new pricing strategies.[1532] The directive represents the first legal act in which 'paying with personal data' is recognised as a counter-performance in business-to-consumer contracting.[1533] As the Commission explains in the recitals, *'[i]n the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money, i.e. by giving access to personal data or other data. [… D]efects of the performance features of the digital content supplied against counter-performance other than money may have an impact on the economic interests of consumers.'*[1534] In other words, consumer protection safeguards should also apply to contracts where consumers actively provide counter-performance other than money in the form of personal data or any other data. Specifically, Articles 13 (2)(c) and 16(4)(b) of the proposed directive on digital content could be a useful alternative to the rights to data portability and access, as they mandate the option for consumers to receive their data for free after they leave the service.[1535]

[1529] Article 3 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OC L 095.

[1530] See for instance Norwegian consumer council, Consumer protection in fitness wearables <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf> accessed 23 may 2018. Recently, the Italian consumer protection authority opened an investigation of Facebook's problematic personal data processing practices. Public note from 6 April 2018 <http://www.agcm.it/stampa/comunicati/9224-ps11112-informazioni-ingannevoli-su-raccolta-e-uso-dati,-avviata-istruttoria-su-facebook.html> accessed 23 May 2018.

[1531] Art. 1 and 2(5)(6) of the Consumer Rights Directive. *Supra* n 498. Also see 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, 12. However, it should be kept in mind that Directive 98/48/EC and Directive 2000/31/EC on e-commerce define an 'information society service' as 'normally provided for remuneration' meaning that that some social media that are for free fall under this directive.

[1532] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634> accessed 26 January 2018.

[1533] Article 3(1) of the proposed Directive gives exchange with data the same status as money*: 'This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data.'* More on the relation to the payments with perosnal data and the right to know the real value of data in Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy - the Right to Know the Value of Your Data' (2017) 34 Computer Law and Security Review. Also see European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' 16-18 <https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf> accessed 13 November 2017.

[1534] 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, Recital 13.

[1535] Ibid., Art. 13c.

As the consumer protection language slowly filters into data protection statutes, some regard should be paid to those less promising aspects of consumer protection law. In particular, the use of mandatory information duties has been criticised as one of the least effective yet widely used consumer protection measures.[1536] By stressing the importance of transparency and intelligibility, the wording of Article 12 echoes typical disclosure clauses in consumer protection law. For example, Article 7 of the directive on consumer rights[1537] uses almost identical wording: '*information shall be legible and in plain, intelligible language*.' Therefore, consumer protection law should not only be used as a workable alternative to data subject rights but also as a lesson about the causes and consequences of an ineffective legal framework.

10.3.2.2.2.2. Competition law

Competition law settles the conditions for a free and unrestricted access to the market, and this should also be the case on the market of (big, personal) data. Through control of data, companies that operate on two-sided markets generate profit and accumulate power.[1538] If one of these companies acquires a dominant position, this might result in unwanted consequences such as tying, anticompetitive agreements, or exploitation of competitors.[1539] Moreover, by taking control over data, dominant data companies may also restrict consumers' choice and control over data.

Negative effects of data dominance and possible reach of competition law have been addressed by academics, policy-makers, and law enforcement.[1540] Because consumer welfare is one of the outcomes of competition law, consumers' privacy, protection of their data, and control over that data should also be factored in. However, competition authorities have been reluctant to accept the privacy argument.[1541] Privacy concerns are not, in and of themselves, within the scope of the intervention of competition authorities.[1542] This does not mean that competition and data protection law could not go hand in hand. In fact, competition law is already echoed in data protection law, specifically in Article 20 on the right to data portability. As mentioned earlier, data portability represents an antitrust measure, as it prevents lock-ins and allows switching between providers.[1543] At the same time, it also

---

[1536] Joasia A. Luzak, 'Passive Consumers vs. the New Online Disclosure Rules of the Consumer Rights Directive' (2015), 1.
[1537] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, [2011] OJ L 304.
[1538] Chapter 2, section 2.3.1. EDPS considers the absence of a clear definition of a primary and a secondary data market a fundamental problem. 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'.
[1539] ibid, 28.
[1540] See for instance Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' [2013] SSRN Electronic Journal 1; Lina Khan, 'Amazon's Antitrust Paradox' 126 Yale Law Journal (January 31, 2017).
In Germany, the antitrust watchdog (Bundeskartellamt) initiated a proceeding against Facebook Inc., USA, in relation to its terms of service on the use of user data. They accuse Facebook of abusing its possibly dominant position in the market for social networks in violation of Article 102 TFEU. Specifically, Bundeskartellamt claims that Facebook is using its position as the dominant social network to illegally track users across the internet and reinforce its might in online advertising. Nicholas Hirst, Facebook's data collection faces antitrust charge in Germany, *politico.eu* (19 December 2017) <https://www.politico.eu/article/facebook-data-collection-could-be-an-antitrust-abuse-in-germany/> accessed 23 May 2018.
[1541] Torsten Körber, 'Is Knowledge (Market) Power ?' [2016] NZKart.
[1542] Ibid., 31.
[1543] Chapter 8, section 8.5.1.

enhances consumers' choice and control, two points at which competition and data protection policy interrelate.

10.3.2.2.2.3. Regulation of AI

In the growing data economy, which relies on the use of AI and machine learning, personal data is treated as a highly valuable source, giving data-driven firms a competitive edge.[1544] To some extent, the GDPR addresses the risks of AI by including new overarching provisions on accountability, fairness, and transparency, along with more tangible requirements such as those concerning the right to explanation of automated decisions, to contest them, and the obligation to carry out privacy impact assessments.[1545] Yet, the GDPR cannot address all the risks imposed by AI. For instance, the question of the limits to what AI systems can suggest to a person based on a construction of the person's own conception of his identity goes beyond the scope of data protection and privacy.[1546]

There seems to be a consensus in the EU that AI should be better regulated. In fact, because of the GDPR's global influence, the EU is particularly well placed to lead the AI debate on the global stage.[1547] Liisa Jaakonsaari, an EU MP, proposed a general framework on algorithmic accountability and transparency that could be the next step in achieving these goals without raising unrealistic expectations towards the right to information in the GDPR.[1548] More recently, the EC published a Communication on AI in which it announced that it plans to address AI risks through new ethical guidelines, with due regard to fundamental rights.[1549] Such guidelines, though less specific and non-binding, may be a useful complement to data protection law in particular in the areas where tangible data protection rules are less effective.

10.3.3. Recommendations

The section above synthesised some possible solutions to enhance data subject rights. Below, these solutions are clustered into three sets of recommendations addressed to the leading actors in the data economy: the industry and the regulators. In my view, all three sets of recommendations are viable strategies to improve thre current situation in terms of user control and to contribute to a more sustainable, fair and, ultimately, individuals-friendly data economy.

1. Leveraging on technology

The industry should continue to investigate technical implementations of the rights to help data subjects exercise control. While doing so, it should be mindful of two facts. First, control settings may prove misleading, promising more than they deliver and creating a false feeling of trust and autonomy. Second, too much control and too many choices may overwhelm and confuse individuals, leading to undesirable results. Regulators should recognise the importance of technology in enhancing data

---

[1544] Chapter 1, section 1.1.
[1545] Articles 5(1)(a), 13(2)(f), 14(2)(f), 15(1)(h) and 22 of the GDPR.
[1546] European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and "Autonomous" Systems', 2018, 11.
[1547] Report from the high level hearing: A European Union strategy for Artificial Intelligence (27 March 2018) < <https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_report_-_hearing_-_a_european_union_strategy_for_artificial_intelligence.pdf> accessed 23 May 3018.
[1548] Liisa Jaakonsaari, 'Who sets the agenda on algorithmic accountability?' *EURACTIV* (26 October 2016). Jaakonsaari also warns of the fact that the right to explnantion only applies to a relatively narrow segment of algorithmic decision-making, as the definition of "solely automated" can be circumvented.
[1549] European Commission, 'Communication from the Commission: Artificial Intelligence for Europe', 2018.

subject control but also be aware of its drawbacks. Technological solutions should be continually reviewed and assessed to check whether they still meet the statutory standards.

2. Applying the control and the protection side of the GDPR in a complementary way

While implementing the GDPR, the industry should continuously seek better connections between data protection duties and data subjects' control measures, keeping in mind that to be effective, control rights must be complemented with data controllers' duties. Regulators supervising the data economy players should be mindful of these interactions and consider data subject rights through the lens of controllers' duties, e.g. privacy by design.

3. Investigating overlaps between data protection and other legal areas, and leveraging them

The data economy players, in particular platforms, should brace themselves for additional and more extensive regulation of their data practices. The regulators should pay attention to the overlaps between different legal domains and consider how they can best complement each other. As shown above, if these multiple instruments are combined smartly, and implemented with prudence and sufficient understanding of the specifics of each legal area, the holistic approach has the potential to heal some of the long-lasting discrepancies in data protection law and strengthen individual control.

Samenvatting (Dutch Summary)

Rechten van betrokkenen en de datagestuurde economie

Door de enorme groei in de hoeveelheid informatie en de toegenomen effectiviteit waarmee informatie kan worden verspreid, zijn (persoons)gegevens een zeer waardevol product geworden. De snellere circulatie van informatie brengt het risico met zich mee dat mensen de controle verliezen over hun persoonsgegevens. Rechten van betrokkenen – te weten het recht op informatie over de verwerking van persoonsgegevens, het recht op gegevenswissing, het recht om bezwaar te maken tegen de verwerking van gegevens, het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit, het recht op inzage, en het recht op overdraagbaarheid van gegevens – maken deel uit van gegevensbeschermingsbepalingen die individuele controle beogen te versterken. In 2018 heeft het Europees Parlement de Algemene verordening gegevensbescherming (AVG) aangenomen. Deze nieuwe verordening heeft tot doel de gegevensbescherming te versterken en aan te passen aan de veranderde context van een geglobaliseerde wereld waarvan de delen onderling verbonden zijn. De wijzigingen leidden tot enkele substantiële verbeteringen van het recht van de betrokkene. Toch lijkt er nog steeds een kloof te bestaan tussen de rechten die betrokkenen volgens deze verordening zouden moeten hebben, en de effectuering van deze rechten in de praktijk. Dit proefschrift onderzoekt of de rechten van betrokkenen onder de AVG effectief zijn in de data-economie en zo niet, hoe deze tekortkomingen kunnen worden weggenomen. Hiertoe onderzoekt het proefschrift de zes bovengenoemde rechten die betrokkenen hebben onder de nieuwe verordening, de implicaties van de datagestuurde economie en hoe zij de controle over gegevens verbeteren.

Het recht op informatie houdt in dat betrokkenen de beschikking hebben over een uitgebreide informatiecatalogus, meestal in de vorm van een 'privacy notice/policy'. De AVG verplicht de informatie aan te bieden in een gebruikersvriendelijke vorm. Met name lijkt het recht op gestandaardiseerde iconen een nieuwe, gebruikersvriendelijke optie te bieden om meer controle uit te oefenen over moderne gegevensstromen. Ondanks deze nieuwe stappen in de AVG lijken de rechten die de wet biedt zwak. In de data-economie lijken psychologische, technologische en economische factoren een negatief effect te hebben op het vermogen van betrokkenen om informatiestromen te begrijpen. Zelfs als verwerkingsverantwoordelijken informatie over alle mogelijke gegevensbestemmingen en het hergebruiken van deze gegevens zou openbaren, zou dergelijke informatie nutteloos zijn als betrokkenen overbelast worden met deze informatie.

Op grond van het *recht op inzage* kan een betrokkene zowel haar persoonlijke gegevens alsook de gegevensbronnen en ontvangers van een specifieke dataset opvragen. Het recht op inzage zorgt er ook voor dat betrokkenen informatie krijgen over logica en de gevolgen van geautomatiseerde verwerking. Dit is cruciaal in de nieuwe economische omgeving waar zelfs routineactiviteiten worden uitgevoerd aan de hand van kunstmatige intelligentie. Het uitleggen van de werking en mogelijke gevolgen van algoritmen is echter gecompliceerd en het recht op inzage heeft slechts een beperkte reikwijdte. Algoritmen kunnen bijvoorbeeld geaggregeerde persoonlijke gegevens gebruiken die niet aan een specifieke persoon kunnen worden toegeschreven. In dergelijke gevallen is het recht op inzage niet van toepassing, maar geanonimiseerde gegevens kunnen nog steeds leiden tot profilering en toezicht.

Het *recht op gegevenswissing* treedt naar voren als één van de sterkste 'controle-rechten'. Gezien vanuit het perspectief van de data-economie is het belangrijk dat betrokkenen in staat zijn gegevens te verwijderen die niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins zijn verwerkt. Het vaststellen van het beginsel van doelbinding is een verbetering, omdat gegevens tegenwoordig steeds meer worden gebruikt voor secundaire doeleinden. In aanvulling op het formele recht op gegevenswissing in artikel 17 van de AVG, kan de effectuering van dit recht worden vergemakkelijkt door middel van andere wettelijke rechten zoals het recht om bezwaar te maken en door de mogelijkheid van het intrekken van toestemming evenals door technische alternatieven zoals houdbaarheidsdata en 'down-ranking'. De context van de bepaling over het vergeetrecht wijst uit dat betrokkenen niet alleen door het recht om vergeten te worden in staat worden gesteld om gegevens te wissen, maar vooral ook door de technologische en sociale omgeving waarbinnen deze controle moet worden uitgeoefend. Zo introduceerde Google een gebruiksvriendelijke interface voor de uitoefening van het recht om vergeten te worden, waarna duizenden gebruikers een verzoek indienden om vergeten te worden. Het recht op gegevenswissing, net als sommige andere bepalingen van de wetgeving inzake gegevensbescherming, verliest echter zijn kracht vanwege een aantal verschillende kenmerken van de data-gestuurde economie, zoals de gewoonte om geanonimiseerde gegevens te hergebruiken. Kopieën van sommige persoonlijke gegevens (bijvoorbeeld 'log records') kunnen bijvoorbeeld in databases van sociale netwerken aanwezig blijven. Hoewel deze verslagen vanwege anonimisering geen persoonlijke identificatiegegevens bevatten, kan het risico op de-anonimisering nooit volledig worden geëlimineerd.

Het *recht op overdraagbaarheid van gegevens (dataportabiliteit)* is een nieuw recht met een nauwgedefinieerd toepassingsbereik die consequenties heeft voor zijn doel. Aan de ene kant kan dataportabiliteit de transparantie van gegevensverwerking vergroten en kan het betrokkenen helpen hun online identiteit te beheren. Aan de andere kant is het recht in de huidige vorm aanzienlijk beperkt en verdere wijzigingen in de regelgeving in artikel 20 zijn op dit moment hoogst onwaarschijnlijk. Dat gezegd hebbende, staat de AVG-versie van het recht op overdraagbaarheid van gegevens niet alleen in de missie om de controle van betrokkenen te verbeteren. Sommige andere juridische domeinen, zoals het mededingingsrecht, bevatten vergelijkbare ideeën over dataportabiliteit die tot positieve resultaten kunnen leiden.

Het recht van bezwaar en het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit, die beide in de AVG zijn neergelegd, beperken de risico's die profilering met zich meebrengt. De bepalingen waarin deze rechten zijn neergelegd bewerkstelligen dat betrokkenen beter controle kunnen uitoefenen op gegevens. Dit gebeurt op diverse manieren, bijvoorbeeld door de expliciete erkenning van profilering als een vorm van verwerking van persoonsgegevens en door het faciliteren van een geschikt technologisch proces. Beide rechten worden echter nog steeds weinig toegepast. De reden hiervan is gelegen in het feit dat mensen vatbaar zijn voor manipulatie, niet geïnteresseerd zijn in het verkrijgen van extra informatie, en zijn belast met enorme hoeveelheden informatie. Bovendien zijn beide rechten onderontwikkeld en dubbelzinnig, en dienen zij in de rechtspraak te worden geïnterpreteerd, hetgeen waarschijnlijk niet in de nabije toekomst zal gebeuren.

In de conclusie worden vijf beginselen van gegevensbescherming besproken, te weten rechtmatigheid en transparantie van verwerking, doelbinding, minimale gegevensverwerking, integriteit en vertrouwelijkheid, en de verantwoordingsplicht. Deze beginselen worden gebruikt als een kader

waarbinnen de doeltreffendheid van de hierboven genoemde rechten kan worden beoordeeld. De beoordeling bevestigt wat uit de eerdere hoofdstukken al was gebleken; in theorie lijkt de verordening een veelbelovende ontwikkeling in te houden, maar deze voldoet in de praktijk niet aan de verwachtingen. Aangezien de data-economie zich naar verwachting zal blijven ontwikkelen, zal naar alternatieve oplossingen moeten worden gezocht om tegemoet te komen aan het gebrek aan individuele controle. Hiertoe worden drie benaderingen voorgesteld om deze individuele controle over persoonsgegevens verder te versterken dan in het huidige systeem van rechten van betrokkenen gebeurt. Ten eerste moeten nieuwe technologische oplossingen worden geïntroduceerd die beginselen zoals privacy, billijkheid en controle bevorderen. Vervolgens moeten de rechten van betrokkenen worden aangevuld met mechanismen ter verruiming van de plichten die de gegevensbeschermingswetgeving oplegt, zoals 'privacy by design'. En tot slot moet de nadruk worden gelegd op het feit dat overlap bestaat tussen gegevensbescherming en andere juridische gebieden.

Bibliography

Alessandro Acquisti, 'From the Economics of Privacy to the Economics of Big Data' (2014) <https://www.heinz.cmu.edu/~acquisti/papers/economics-big-data-acquisti-lane-book.pdf> accessed 25 August 2018.

Albrecht JP, 'Hands Off Our Data!' <https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf>

Alhadeff J, Van Alsenoy B and Dumortier J, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in D Guagnin, L Hempel and C Ilten (eds), *Managing Privacy throughAccountability* (Palgrave Macmillan 2012)

Altaweel I, Good N and Hoofnagle CJ, 'Web Privacy Census' [2015] Journal of Technology Science <https://techscience.org/a/2015121502>

Andrejevic M and Gates K, 'Big Data Surveillance: Introduction' (2014) 12 Surveillance & Society 185

Androcec D, 'Data Portability among Providers of Platform as a Service' [2013] Research Papers, Faculty Of Materials Science And Technology In Trnava, Slovak University Of Technology In Bratislava <https://www.mtf.stuba.sk/buxus/docs/doc/casopis_Vedecke_prace/32SN/002_Androcec.pdf>

Article 29 Data Protection Working Party, 'Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data on-Line in the European Union' (2001)

——, 'Opinion 02/2013 on Apps on Smart Devices'(2013)

——, 'Opinion 1/2010 on the Concepts Of "controller" and "processor"' (2010)

——, 'Working Document on Data Protection Issues Related to RFID Technology' (2005)

——, 'Opinion 4/2007 on the Concept of Personal Data' (2007)

——, 'Opinion 2/2010 on Online Behavioural Advertising' (2010)

——, 'Opinion 15/2011 on the Definition of Consent' (2011)

——, 'Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2011)

——, 'Opinion 03/2013 on Purpose Limitation' (2013)

——, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (2013)

——, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12' (2014)

——, 'Opinion 05/2014 on Anonymisation Techniques' (2014)

——, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014)

——, ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679’ (2018)

——, ‘Guidelines on the Right to Data Portability’ (2016)

——, ‘Guidelines on the Right to Data Portability’ (2017)

——, ‘Opinion 2/2017 on Data Processing at Work’ (2017)

——, ‘Guidelines on Consent under Regulation 2016/679’ (2018)

——, ‘Guideines on Transparency under Regulation 2016/679’ (2018)

Atkinson JA and others, ‘Combining Semi-Automated Image Analysis Techniques with Machine Learning Algorithms to Accelerate Large-Scale Genetic Studies’ (2017) 6 (10) GigaScience 1

Ausloos J, ‘The “Right to Be Forgotten” - Worth Remembering?’ (2012) 28 Computer Law and Security Review 143

Ausloos J and Dewitte P, ‘Shattering One-Way Mirrors – Data Subject Access Rights in Practice’ (2018) 8 International Data Privacy Law

Bachlechner D and others, ‘WP1 Mapping the Scene: D1.2 Report on the Analysis of Framework Conditions (Deliverable for the EuDEco H2020 Project)’ (2015) <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/d1.2_analysisoframeworkconditions-v1_2015-08-31-1.pdf>

Balkin JM, ‘Free Speech Is a Triangle’ (2018) 118 Columbia Law Review 7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186205>

Balkin JM, ‘Information Fiduciaries and the First Amendment’ (2016) 49 U.C. Davis Law Review 1183

Barnard C and Peers S, *European Union Law* (Oxford University Press 2017)

Barocas S and Selbst A, ‘Big Data’s Disparate Impact’ (2016) 104 California law review 671

Bartevyan L, ‘DLG-Expert report 5/2015: Industry 4.0 – Summary Report’ (2015) <https://www.cenit.com/fileadmin/dam/Corporate/PDFs/2015_5_Expertenwissen_E.pdf>

Bartolini C and Siry L, ‘The Right to Be Forgotten in the Draft Data Protection Regulation’ (2016) 32 Computer Law & Secrity Review 2

Bayamlıoğlu E, ‘Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation’ (2018) <https://ssrn.com/abstract=3097653>

Beitz CR, *The Idea of Human Rights* (Oxford University Press 2009)

Ben-Shahar O and Schneider C, *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014)

Bernasek A and Mongan DT, *All You Can Pay* (Nation Books 2015)

Bijsterveld S van, 'A Crucial Link in Shaping the New Social Contract between the Citizen and the EU' in PJ Stolk (eds), *Transparency in Europe II: Public Access to Documents in the EU and its Member States* (Ministry of the Interior and Kingdom Relations Constitutional 2004)

Bird & Bird, 'Guide to the General Data Protection Regulation' (2017) <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>

Bond RM and others, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489 Nature 295 <http://dx.doi.org/10.1038/nature11421>

Bonnici JPM, 'Exploring the Non-Absolute Nature of the Right to Data Protection' (2014) 28 International Review of Law, Computers & Technology 131 <https://doi.org/10.1080/13600869.2013.801590>

Bosco F and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in S Gutwirth, R Leenes and P de Hert (eds), *Reforming European Data Protection Law* (2015)

Bouguettaya ARA and Eltoweissy MY, 'Privacy on the Web: Facts, Challenges, and Solutions' (2003) 1 IEEE Security & Privacy 40

Brandimarte L, Acquisti A and Loewenstein G, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4 Social Psychological and Personality Science 4(3) 340

British Academy and the Royal Society, 'Data Management and Use: Case Studies of Technologies and Governance' (2017) <https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-case-studies.pdf>

Brkan M, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23 Maastricht Journal of European and Comparative Law 812

Brockhoff J and others, 'Google/DoubleClick: The First Test for the Commission's Non- Horizontal Merger Guidelines' (2008) Competition Policy Newletter 53

Brown I and Marsden C, 'Regulating Code: Towards Prosumer Law?' (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2224263>

Brownsword R, 'In the Year 2061: From Law to Technological Management' (2015) 7 Law, Innovation and Technology 1

——, 'Technological Management and the Rule of Law' (2016) 8 Law, Innovation and Technology 100

Brouwer E and Borgesius Zuiderveen F, 'Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. and M. and S. judgment (C-141/12 and C-372/12), case report' (2015) European Journal of Migration and Law 17

Bruce Schneier, *Data and Goliath* (WWNorton & Company 2015)

Brulc U, 'Do kod seže pravica seznanitve z lastnimi osebnimi podatki?' [2016] 47 Pravna praksa 6

Brunton F and Nissenbaum HF, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press 2016)

Búrca G de, 'The Road Not Taken: The EU as a Global Human Rights Actor' (2011) 105 American Journal of International Law 649

Burger JM, 'Negative Reactions to Increases in Perceived Personal Control' (1989) 56 Journal of Personality and Social Psychology 246

Burri M and Schär R, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479

Bygrave LA, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Report 17

Bygrave LA, 'Data Privacy Law and the Internet: Policy Challenges' in D Lindsay and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014)

——, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International 2002)

Caliskan A, Bryson JJ and Narayanan A, 'Semantics Derived Automatically from Language Corpora Contain Human-like Biases' (2017) 356 Science 183

Calo R, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law Journal 1131

——, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350>

Campbell AV, 'Human Dignity and Commodification in Bioethics' in D Mieth and others (eds), *The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives* (Cambridge University Press 2014)

Caplan R, Hanson L and Donovan J, 'Dead Reckoning: Navigating Content Moderation After "Fake News"' (Data & Society Research Institute 2018) <https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf>

Cate FH, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of the Infomation Economy (2006)* (Routledge 2006)

Cattaneo G and others, 'European Data Market SMART 2013 / 0063 D8 — Second Interim Report The Data Market in the World' (IDS 2014) <https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report_030417_2.pdf>

Centre for Information Policy Leadership, 'Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR' (2017) <https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf> accessed 17 November 2017

Chalmers D, Davies G and Monti G, *European Union Law: Cases and Materials* (Cambridge University Press 2010)

Chirita AD, 'The Rise of Big Data and the Loss of Privacy' in M Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer 2018)

Christin A, Rosenblat A and Boyd D, 'Courts and Predictive Algorithms' (2015) Data & Civil Rights: A New Era of Policing and Justice <http://www.law.nyu.edu/sites/default/files/upload_documents/Angele Christin.pdf>

Clavell GG, 'Policing, Big Data and the Commodification of Security' in B Van Der Sloot, D Broeders and E Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016)

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness Data Protection and the Role of Fairness' (2017) 29 CiTiP Working Paper Series

Cohen JE, 'What Privacy Is for' (2012) 126 Harvard Law Review 1904

——, 'Affording Fundamental Rights' (2017) 4 Critical Analysis of Law

——, 'Law for the Platform Economy' (2017) 35 U.C. Davis Law Review 133

——, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1

Competition and Markets Authority, 'The Commercial Use of Consumer Data' (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf>

Cooke E, *Land Law* (Oxford University Press 2012)

Coorevits P and others, 'Electronic Health Records: New Opportunities for Clinical Research' (2013) 274 Journal of Internal Medicine 547

Cormack A, 'GDPR: What's Your Justification?' (JISC community, 13 October 2017) <https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification>

Coudert F, Dumortier J and Verbruggen F, 'Applying the Purpose Specification Principle in the Age of "big Data": The Example of Integrated Video Surveillance Platforms in France' (2012) ICRI Research Paper 6/2012 < https://lirias2repo.kuleuven.be/bitstream/id/216838/>

Craig P and De Burca G, *EU Law: Text, Cases, and Materials* (Oxford University Press 2015)

Cranor LF, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2011) 10 Journal on Telecommunication & High Technology Law 273

Crawford K and Schultz J, 'Big Data and Due Process - Toward a Framework To Redress Predictive Privacy Harms' (2014) 55 BCL Rev. 93

Crootof R, 'An Internet of Torts' (2018) <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Crootof-An-Internet-of-Torts-We-Robot-Submission.pdf>

Custers B, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Wolf Legal Publishers 2004)

——, ‘Data Dilemmas in the Information Society’ in Custers B and others (eds), *Discrimination and Privacy in the Information Society* (Springer 2013)

Custers B, ‘Click Here to Consent Forever: Expiry Dates for Informed Consent’ (2016) 3 Big Data & Society

Custers B and Bachlechner D, ‘Advancing the EU Data Economy: Conditions for Realizing the Full of Potential of Data Reuse’ [2018] 22 (4) Information Polity

Custers B and Ursic H, ‘Worker Privacy in a Digitalized World under European Law’ 39 Comparative Labor Law & Policy Journal 323

Custers B and Ursic H, ‘Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection’ (2016) 6 *International Data Privacy Law* 1

Custers B, van der Hof S and Schermer B, ‘Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law’ (2013) 10 SCRIPTed

Daly A, ‘The Internet, User Autonomy and EU Law’ (2016) <https://www.ssrn.com/abstract=2780789>

Data Protection Network, ‘Guidance on the Use of Legitimate Interests under the EU General Data Protection Regulation’ (2017) <https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf>

Davies T, ‘Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies’ in LM Aiello and D McFarland (eds), *Social Informatics: Proceedings of the 6th International Conference* (Barcelona, 2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2507608>

Davis K, *Ethics of Big Data* (O’Reilly Media 2012)

Davison MJ, *The Legal Protection of Databases* (Cambridge University Press 2008)

De Filippi P, ‘Big Data, Big Responsibilities’ (2014) 3 Internet Policy Review

De Hert P and others, ‘The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services’ (2018) 34 Computer Law & Security Review 193

De Hert P and Gutwirth S, ‘Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power’ in E Claes, A Duff and S Gutwirth (eds), *Privacy and the criminal law* (Intesentia 2006)

——, ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

De Hert P and Lammerant H, ‘Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever?’ in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016)

Den Hertog L, ‘The Rule of Law in the EU: Understandings, Development and Challenges’ (2012) 53 Acta Juridica Hungarica 204

Directorate General for Internal Policies, 'Big Data and Smart Devices and Their Impact on Privacy' (European Parliament 2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf>

Doyle D, Tsymbal A and Cunningham P, 'A Review of Explanation and Explanation in CaseBased Reasoning' <https://scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-41.pdf> accessed 27 December 2018.

Drexl J and others, 'Position Statement of the Max Planck Institute for Innovation and Competition on the European Commission's "Public Consultation on Building the European Data Economy"' (Max Planck Institute for Innovation and Competition, 2017) <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf>

Ecommerce Europe, 'Position Paper Privacy and Data Protection; Safety and Transparency for Trust and Consumer Centrality' (2014) <https://www.ecommerce-europe.eu/app/uploads/2016/07/ecommerce-europe-position-paper-privacy-and-transparency-for-consumer-trust-and-consumer-centricity.pdf.pdf>

Edwards L and Abel W, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors' (2014) CREATe Working Paper 2014/15

Edwards L and Veale M, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for (2017) 16 Duke Law and Technology Review

Engels B, 'Data Portability among Online Platforms' (2016) 5 Internet Policy Review Journal on internet regulation 1

ENISA, 'Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems' (2015) <https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport>

Esposito E, 'Algorithmic Memory and the Right to Be Forgotten on the Web' (2017) 4 Big Data & Society

European Banking Federation, 'European Banking Federation's Comments to the Working Party 29 Guidelines on the Right to Data Portability' (2017) <http://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf>

European Commission, 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Business' <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>

——, 'ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation - Final Report' (2015) <https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>

——, ‘How Does the Data Protection Reform Strengthen Citizens’ Rights?’ (2016) <ec.europa.eu/newsroom/just/document.cfm?doc_id=41525>

——, ‘Factsheet on the “Right to Be Forgotten" ruling’ <http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf>

European Commission Staff, ‘Online Platforms - Accompanying the Document Communication Communication on Online Platforms and the Digital Single Market’ (2016)

——, ‘Online Platforms - Accompanying the Document Communication on Online Platforms and the Digital Single Market {COM(2016) 288}’ (2016)

European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the Data Protection Reform Package’ (2012) <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf>

——, ‘Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy’ (2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 12 November 2017

——, ‘Opinion 7/2015 Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability (2015)’

——, ‘Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology’ (2015)

——, ‘Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content’ (2017)

——, ‘Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content’ (2017)

European Group on Ethics in Science and New Technologies ‘Statement on Artificial Intelligence, Robotics and “Autonomous” Systems’ (2018) <http://www.unapcict.org/ecohub/statement-on-artificial-intelligence-robotics-and-autonomous-systems/at_download/attachment1>

European Union Agency for Fundamental Rights and Union, ‘Freedom to Conduct Business - Exploring the Dimensions of a Fundamental Right’ (2015)

European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Non-Discrimination Law* (2011)

——, *Handbook on European Data Protection Law* (2014)

European Union Agency for Network and Information Security, ‘Privacy and Data Protection by Design – from Policy to Engineering’ (2014)

Evans A, ‘Subject Access Requests: Fishing for Information?’ (Gateley Plc, 2015) <http://gateleyplc.com/wp-content/uploads/2016/01/Subject-Access-Requests-fishing-for-information.pdf>

Executive Office of the President (White House), 'Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights' (2016) <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>

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

Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> accessed 12 November 2017

Federal Trade Commission, 'Data Brokers - A Call for Transparency and Accountability' (2014) <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

——, 'Internet of Things: Privacy & Security in a Connected World' (2015) <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Ferrara L, 'Working Document on Establishment of an EU Mechanism on Democracy, the Rule of Law and Fundamental Rights - Litigation by Citizens as a Tool for Private Enforcement' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-575.319+01+DOC+PDF+V0//EN&language=EN>

Ferretti F, *EU Competition Law, the Consumer Interest and Data Protection - The Exchange of Consumer Information in the Retail Financial Sector* (Springer 2014)

Fialová E, 'Data Portability and Informational Self-Determination' (2014) 8 Masaryk University Journal of Law and Technology 45

Finck M, 'Blockchains and Data Protection in the European Union' (2017) Max Planck Institute for Innovation and Competition Research Paper 18/1

——, 'Blockchain Regulation' [2018] German Law Journal

Fischer-Hübner S and others, 'Online Privacy: Towards Informational Self-Determination on the Internet' in Mireille Hildebrandt and others (eds), *Digital Enlightenment Yearbook 2013* (2013)

Food and Drug Administration, Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices - Guidance for Industry and Food and Drug Administration Staff Document (31 August 2017) <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm513027.pdf>

Forbrukerradet, 'Consumer Protection in Fitness Wearables' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-

protection-in-fitness-wearables-forbrukerradet-final-version.pdf>

Forbrukerrådet, 'Appfail? Threats to Consumers in Mobile Apps' (2016)

Ford RA and Price WN, 'Privacy and Accountability in Black-Box Medicine' (2016) 23 Michigan Telecommunications and Technology Law Review

Fosch Villaronga E, Kieseberg P and Li T, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right To Be Forgotten' [2017] Computer Security & Law Review

Frankfurt HG, 'Alternate Possibilities and Moral Responsibility' (1969) 66 The Journal of Philosophy 829

Frosio GF, 'Right to Be Forgotten: Much Ado about Nothing' (2017) 15 Colorado Colorado Technology Law Journal 307

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014)

Future of Privacy Forum and The Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (2011) <https://fpf.org/wp-content/uploads/Best-Practices-for-Mobile-App-Developers_Final.pdf>

Geambasu R and others, 'Vanish: Increasing Data Privacy with Self-Destructing Data', *Proc. of the 18th USENIX Security Symposium* (2009)

Géczy P, 'Data Economy Dimensions' (2015) 9 Global Journal of Business Research

Gellert R, 'Understanding Data Protection as Risk Regulation' (2015) 18 Journal of Internet Law 3

Geradin D, 'Data Portability and EU Competition Law' (*Presentation at the BITS conference*, 2014)

Geradin D and Kuschewsky M, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088>

Gigerenzer G and Selten R, *Bounded Rationality: The Adaptive Toolbox* (MIT Press 2002)

Global Future Council on Human Rights 2016-2018 (World Economic Forum), 'How to Prevent Discriminatory Outcomes in Machine Learning' (2018)

Goodman B and Flaxman S, 'European Union Regulations on Algorithmic Decision-Making and A "right to Explanation"' (2016) <http://arxiv.org/abs/1606.08813>

Graef I, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (2015) 39 Telecommunications Policy 502

——, 'Blurring Boundaries of Consumer Welfare How to Create Synergies between Competition, Consumer and Data Protection Law' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881969>

Graux H, Ausloos J and Valcke P, 'The Right to Be Forgotten in the Internet Era' in J Pérez, E Badía and

R Sáinz Peña (eds), *The Debate on Privacy and Security over the Network: Regulation and Markets* (Ariel 2012)

Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books, 2014)

Group WEF in collaboration with BC, 'Unlocking the Value of Personal Data: From Collection to Usage' (World Economic Forum 2013)

Groussot X, Pétursson GT and Pierce J, 'Weak Right, Strong Court - The Freedom to Conduct Business and the EU Charter of Fundamental Rights' in Douglas-Scott and Hatzis (eds), *Research Handbook on EU Law and Human Rights* (Edward Elgar Publishing Ltd 2017)

Gubbi J and others, 'Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions' (2013) 29 Future Generation Computer Systems 1645

Gürses S and Hoboken J Van, 'Privacy After the Agile Turn' in J Polonetsky, O Tene and E Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017)

Gutwirth S and Hildebrandt M, 'Some Caveats on Profiling' in S Gutwirth, Y Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010)

Haber E, 'Privatization of the Judiciary' (2016) 40 Seattle University Law Review 115

Hacker P and Petkova B, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers' (2017) 15 Northwestern Journal of Technology and Intellectual Property 1

Hallinan D and others, 'PRESCIENT Deliverable 3: Privacy, Data Protection and Ethical Issues in New and Emerging Technologies: Assessing Citizens' Concerns and Knowledge of Stored Personal Data' (2012)

Hannák A and others, 'Measuring Personalization of Web Search' <https://arxiv.org/pdf/1706.05011.pdf>

Hargittai E, 'Whose Space? Differences Among Users and Non-Users of Social Network Sites' (2008) 13 Journal of Computer-Mediated Communication Whose 276

Hartzog W, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018)

Hartzog W and Rubinstein I, 'The Anonymization Debate Should Be About Risk, Not Perfection' (2017) 60 Communications of the ACM 22

Hatlen LM, 'Conciseness in Legal Writing' [2009] Wisconsin Lawyer, the official publication of the State Bar of Wisconsin

Haut L, Brinkmann M and Abels S, 'WP2 Developing the Initial Model: D2.4 Report on the Technological Analysis (Deliverable for the Eudeco H2020 Project)' (2016) <http://data-reuse.eu/wp-content/uploads/2016/06/D2.4_ReportOnTheTechnologicalAnalysis-v1_2016-02-29.pdf>

Hearn WE, Theory of legal duties and rights (1883)

Helberger N, ‘Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law’ <https://www.ivir.nl/publicaties/download/1747.pdf>

Helberger N, Zuiderveen Borgesius FJ and Reyna A, ‘The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law’ (2017) 54 Common Market Law Review

Helbing D, ‘Economy 4.0 and Digital Society: The Participatory Market Society Is Born (Chapter 8 of Digital Society)’ (2014) Digital Society <http://papers.ssrn.com.ezproxy.liv.ac.uk/sol3/papers.cfm?abstract_id=2539330>

Hijmans H, ‘The European Union as a Constitutional Guardian of Internet Privacy and Data Protection’ (PhD Thesis, University of Amsterdam 2016)

Hildebrandt M, ‘Defining Profiling: A New Type of Knowledge?’ in Hildebrandt Mireille and Gutwirth Serge (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

——, ‘The Dawn of a Critical Transparency Right for the Profiling Era’ in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012)

——, ‘Slaves to Big Data. Or Are We?’ [2013] IDP Revista De Internet, Derecho Y Política

——, ‘Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning’ (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081776>

Hintze M, ‘In Defense of the Long Privacy Statement’ (2015) 76 Maryland Law Review 1044

Hoofnagle CJ and Urban JM, ‘Alan Westin’s Privacy Homo Economicus’ (2014) 49 Wake Forest L. Rev. 261

Hornung G and Schnabel C, ‘Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination’ (2009) 25 Computer Law and Security Review 84 <http://dx.doi.org/10.1016/j.clsr.2008.11.002>

Hu R and others, ‘Bridging Policy, Regulation and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR’ in Ronald Leenes and others (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017)

Hurley M and Adebayo J, ‘Credit Scoring in the Era of Big Data’ (2016) 18 Yale Journal of Law and Technology 148

Hustinx P, ‘EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation’ <https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf>

——, ‘European Leadership in Privacy and Data Protection’ (2015) <https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf>

Informacijski pooblaščenec Republike Slovenije, ‘Kdaj Lahko Uporabimo Piškotke? Smernice Informacijskega Pooblaščenca’ <https://www.ip-

rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf>

International Chamber of Commerce UK, 'ICC UK Cookie Guide' (November 2012) <https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf>

Irion K and others, 'A Roadmap to Enhancing User Control via Privacy Dashboards' (IViR Amsterdam, 2017) <https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf>

Irion K and Luchetta G, 'Online Personal Data Processing and EU Data Protection Reform' (Centre for European Policy Studies Brussels 2013)

Jagielska M and Jagielski M, 'Are Consumer Rights Human Rights?' [2012] European consumer protection: theory and practice 336

Jones ML, *CTRL + Z: The Right to Be Forgotten* (NYU Press 2016)

Kahin B, 'Digitization and the Digital Economy' (2016) <http://ssrn.com/abstract=2782906>

Kaltheuner F and Bietti E, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2017) 2 Journal of Information Rights, Policy and Practice

Kamara I, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology 1

Kamarinou D and others, 'Machine Learning with Personal Data Machine Learning with Personal Data' [2016] Queen Mary School of Law Legal Studies Research Paper No. 247/2016.

Kamiran F and Calders T, 'Data Preprocessing Techniques for Classification without Discrimination' (2012) 33 (1) Knowledge and Information Systems 1

Kamleitner B and Mitchell V-W, 'Can Consumers Experience Ownership for Their Personal Data? From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints BT - Psychological Ownership and Consumer Behavior' in Joann Peck and Suzanne B Shu (eds) *Psychological Ownership and Consumer Behaviour* (Springer International Publishing 2018)

Kanala U and Sandhya R, Hadoop Technology for BigData Analytics <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3168340> accessed 27 December 2018.

Kaplan B, 'Selling Health Data: De-Identification, Privacy, and Speech' (2015) 24 Cambridge quarterly of healthcare ethics 256

Danielle Keats Citron, 'Technological Due Process' 85 Washington University Law Review 1249.

Keller D, 'Intermediary Liability and User Content Under Europe's New Data Protection Law' [2015] The Center for Internet and Society 8.

Kerber W, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection and Data Protection' (2016).

Kerr I and Earle J, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65

Khan LM, 'Amazon's Antitrust Paradox' (2017) 126 Yale Law Journal 710

Kindt EJ, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013)

Klonick K, 'The New Governors The People, Rules, And Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598

Kochenov D, Magen A and Pech L, 'Introduction: The Great Rule of Law Debate in the EU' (2016) 54 Journal of Common Market Studies 1045

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law

Koops B-J, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice' (2011) 8 SCRIPTed

——, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipu023>

——, 'A Typology of Privacy' (2016) 38 University of Pennsylvania Journal of International Law

Körber T, 'Is Knowledge (Market) Power?' [2016] NZKart 303; 348

Korenhof P and others, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data' in S Gutwirth, R Leenes and P de Hert (eds) *Reforming European Data Protection Law* (Springer Netherlands 2015)

Kord Davis, *Ethics of Big Data* (O'Reilly Media, Inc 2012)

Korff D, 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws' (2002) <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE>

Kosinski M, Stillwell D and Graepel T, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110 Proceedings of the National Academy of Sciences of the United States of America 5802 <http://www.ncbi.nlm.nih.gov/pubmed/23479631>

Kosta E, *Consent in European Data Protection Law* (Nijhoff 2013)

Kosta E and Stuurman K, 'Technical Standards and the Draft General Data Protection Regulation' in Panagiotis Delimatsis (ed), *The Law, Economics and Politics of International Standardisation* (Cambridge University Press 2017)

Herke Kranenborg, 'Article 8', in Peers a.o. (eds) *The EU Charter of Fundamental Rights. A Commentary* (Hart Publishing 2014)

Kroll J and others, 'Accountable Algorithms' [2016] University of Pennsylvania Law Review 633

Kuczerawy A and Ausloos J, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Colorado Technology Law Journal 219

Kulk S and Borgesius FZ, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in

Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018)

Kulk S and Zuiderveen Borgesius FJ, 'Freedom of Expression and "Right to Be Forgotten" Cases in the Netherlands After Google Spain' (2015) 1 European Data Protection Law Review 113

Kuner C, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2012)

Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2015) Society and Economy Working Paper Series, The London School of Economics and Political Science 3/2015

Kusner M and others, 'Counterfactual Fairness', *1st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA* (2017)

Lambiotte R and Kosinski M, 'Tracking the Digital Footprints of Personality' (2014) 102 Proceedings of the IEEE 1934

Lautenbach G, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press 2014)

Lazaro C and Métayer D Le, 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPT-ed 4

Le Grand G, Polonetsky J and LaFever G, 'GDPR Data Analytics Webinar Summary Three Key Points' (2017) <https://www.anono.com/hubfs/Whitepapers/GDPR_Data_Analytics_Webinar_Summary_Anonos.pdf?t=1507182920438&utm_campaign=Data Analytics under the GDPR &utm_source=hs_email&utm_medium=email&utm_content=57043368&_hsenc=p2ANqtz-9mifrSF5kE2AIJJGqFWy8cpF>

Lee CH and Yoon H-J, 'Medical Big Data: Promise and Challenges' (2017) 36 Kidney Research and Clinical Practice 3

Lessig L, *Code: Version 2.0* (Basic Books 2006)

Levi L, 'Real "Fake News" and Fake "Fake News"' (2018) 16 First Amendment Law Review

Liliya Pullmann and others, 'WP3 Test of the Model; D3.2 Test Report (Deliverable for the EuDEco H2020 Project)' (2017) <http://data-reuse.eu/wp-content/uploads/2017/09/Test-report-final.pdf>

Lisboa PJG, 'Interpretability in Machine Learning – Principles and Practice' in F Masulli, G Pasi and R Yager (eds), *Fuzzy Logic and Applications. WILF 2013.* (Springer International Publishing 2013)

Lunshof JE, Church GM and Prainsack B, 'Raw Personal Data: Providing Access' (2014) 343 Science 373 LP

Lupton D, 'Personal Data Practices in the Age of Lively Data' in J Daniels, K Gregory and T McMIllan Cottom (eds), *Digital Sociologies* (2015)

Luzak JA, 'Passive Consumers vs. the New Online Disclosure Rules of the Consumer Rights Directive' (2015) 2

Lynskey O, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the Eu Legal Order' (2014) 63 International and Comparative Law Quarterly 569

——, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

——, 'Aligning Data Protection Rights with Competition Law' [2017] London School of Economics (LSE) Research Online <http://eprints.lse.ac.uk/80859/>

Lyon D, 'Surveillance, Power and Everyday Life' in R Mansell and others (eds), *Oxford Handbook of Information and Communication Technologies* (Oxford University Press 2007)

Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information & Communications Technology Law 146

Madden M and others, 'Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans' (2017) 95 Washington University Law Review

Malgieri G and Custers B, 'Pricing Privacy - the Right to Know the Value of Your Data' (2017) 34 Computer Law and Security Review

Mantelero A, 'The Future of Consumer Data Protection in the E.U. Re-Thinking The "notice and Consent" paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law and Security Review 643

Margaretta J, 'Why Business Models Matter' *Harvard Business Review* (May 2002)

Marx V, 'The Big Challenges of Big Data' (2013) 498 Nature 255

Mayer-Schönberger V, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2011)

Mayer-Schönberger V and Cukier K, *Big Data a Revolution That Will Transform How We Live, Work and Think* (Mariner Books 2014)

McDermott Y, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017) 4 Big Data & Society

McKinsey, 'Big Data: The next Frontier for Innovation, Competition, and Productivity' (2011) <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx>

——, 'Consumer Marketing Analytics Center' (2012) <https://www.mckinsey.com/~/media/mckinsey/industries/retail/how we help clients/big data and advanced analytics/cmac creating competitive advantage from big data.ashx>

Mendoza I and Bygrave LA, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855>

Mitrou L and Karyda M, 'EU's Data Protection Reform and the Right to Be Forgotten - A Legal Response to a Technological Challenge?' (2012) 5th International Conference of Information Law and Ethics 2012, Corfu-Greece, June 29-30, 2012 <http://www.icsd.aegean.gr/website_files/proptyxiako/388450775.pdf>

Mittelstadt B, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy and Technology

Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (2014) <https://www.debrauw.com/wp-content/uploads/NEWS - PUBLICATIONS/Moerel_oratie.pdf>

Moerel L and Prins C, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' [2016] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123>

Moerel L and van der Wolk A, 'Big Data Analytics under the EU General Data Protection Regulation' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006570>

Morey T, Forbath T and Allison S, 'Customer Data: Designing for Transparency and Trust' *Harvard Business Review* (May 2015)

Narayanan A and Shmatikov V, 'De-Anonymizing Social Networks' (2009) 30th IEEE Symposium on Security and Privacy, 2009.

Newman N, 'Search, Antitrust and the Economics of the Control of User Data' (2014) 31 Yale Journal on Regulation

Nissenbaum H, 'Privacy as Contextual Integrity' [2004] Washington Law Review 119

——, *Privacy in Context* (Stanford University Press 2010)

——, 'A Contextual Approach to Privacy Online' (2011) 140 Dædalus, the Journal ofthe American Academy of Arts & Sciences 32

O'Neil C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016)

O'Neil C and Mann G, 'Hiring Algorithms Are Not Neutral' *Harvard Business Review* (9 December 2016)

Obar JA and Oeldorf-Hirsch A, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016

OECD, 'Exploring Data-Driven Innovation as a New Source of Growth' (2013)

——, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) <http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en>

Oerlemans JJ, 'Investigating Cybercrime' (PhD Thesis, Leiden University 2016).

Ohm P, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2010) 57 UCLA Law Review 1701

Olswang, ‘EU Data Protection Reform: Where Are We – and What Can You Do to Prepare?’ <http://www.cms-lawnow.com/-/media/nabarro-olswang-pdfs/olswang_s_top_12__eu_data_protection_reform.pdf?la=en&hash=71596D1B93E06AEF24A2BD2F529A514473975501>

Oostveen M, ‘Identifiability and the Applicability of Data Protection to Big Data’ [2016] 6 (4) International Data Privacy Law

Osbeck M, ‘What is “Good Legal Writing” and Why Does It Matter?’ (2012) 4 Drexel Law Review 417

Oshana M, ‘Autonomy and the Question of Authenticity’ (2007) 33 Social Theory and Practice

Pariser E, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin Press 2011)

Pasquale F, *The Black Box Society* (Harvard University Press 2015)

Pedreshi D, Ruggieri S and Turini F, ‘Discrimination-Aware Data Mining’, *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining* (ACM 2008)

Peers S and others, *The Eu Charter of Fundamental Rights: A Commentary* (Hart 2014)

Peguera M, ‘The Shaky Ground of the Right to Be Delisted’ (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 507

Politou E et al., ‘Backups and the right to be forgotten in the GDPR: An uneasy relationship' (2018) Computer Law & Security Review: The International Journal of Technology Law and Practice.

Penney JW, ‘Chilling Effects: Online Surveillance and Wikipedia Use’ (2016) 31 Berkeley Technology Law Journal

Poikola A, Kuikkaniemi K and Honko H, ‘MyData – A Nordic Model for Human-Centered Personal Data Management and Processing’ (Finnish Ministry of Transport and Communications) <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y>

Porat A and Strahilevitz LJ, ‘Personalizing Default Rules and Disclosure With Big Data’ (2014) 112 Michigan Law Review 1417

Post RC, ‘Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of The Public Sphere’ (2014) 67 Duke Law Journal 981

Powles J and Hodson H, ‘Google DeepMind and Healthcare in an Age of Algorithms’ (2017) 7 Health and Technology 351

Purtova N, ‘Property Rights in Personal Data: Learning from the American Discourse’ (2009) 25 Computer Law & Security Review 507

Purtova N, 'Property in Personal Data' (PhD thesis, Tilburg University 2011)

——, ‘The Illusion of Personal Data as No One’s Property’ (2013) 7 Law, Innovation, and Technology 83

——, ‘The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law’ (2018) 10 Law, Innovation and Technology

Purtova N, Kosta E and Koops B-J, ‘Laws and Regulations for Digital Health’ in Samuel A Fricker, Christoph Thuemmler and Anastasius Gavras (eds), *Requirements Engineering for Digital Health* (Springer 2014)

Puschmann C and Burgess J, ‘The Politics of Twitter Data’ in K Weller and others (eds), *Twitter and Society* (Peter Lang Publishing, Inc 2014)

Quane H, ‘A Further Dimension to the Interdependence and Indivisibility of Human Rights?: Recent Developments Concerning the Rights of Indigenous Peoples’ (2012) 25 Harvard Human Rights Journal 55

Rao N, ‘Three Concepts of Dignity in Constitutional Law’ (2013) 86 Notre Dame Law Review 183

Raz J, ‘Human Rights in the New World Order’ (2009) 9175 <http://lsr.nellco.org/columbia_pllt%5Cnhttp://lsr.nellco.org/columbia_pllt/9175>

Reidenberg J and others, ‘Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding’ (2015) 30 (1) Berkeley Technology Law Journal 39

Reviglio U, ‘A Right to Internet Serendipity? An Alternative Way to Tackle the Threats of an over-Personalized Internet Experience’ The 2016 Internet, Policy & Politics Conference, Oxford Internet Institute, University of Oxford (2016) <http://ipp.oii.ox.ac.uk/sites/ipp/files/documents/Internet%2520Serendipity.Reviglio.Oxford.pdf>

Rhoen M, ‘Big Data and Consumer Participation in Privacy Contracts: Deciding Who Decides on Privacy’ (2015) 31 Utrecht Journal of International and European Law 51

——, ‘Beyond Consent: Improving Data Protection through Consumer Protection Law’ (2016) 5 Internet Policy Review

Richards NM and King JH, ‘Three Paradoxes of Big Data’ (2013) 66 Stan. L. Rev. Online <https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/>

——, ‘Big Data Ethics’ (2014) 49 Wake Forest Law Review 393

Robinson N and others, ‘Review of the European Data Protection Directive’ (2009) <https://www.rand.org/pubs/technical_reports/TR710.html>

Rodotà S, ‘Data Protection as a Fundamental Right’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

Röhsner M, ‘Data Portability as a Service; A Legal and Normative Analysis of the Requirements under the Law of the European Union for Contracts That Authorize a Service Provider to Exercise the Right to Data Portability on Behalf of a Data Subject’ (Master's Thesis, Leiden University 2017)

Rosen J, 'The Right to Be Forgotten' [2012] Stanford Law Review Online 88 <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>

Rouvroy A and Poullet Y, '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)

Rubinstein IS, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74

Rustad ML and Kulevska S, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28 Harvard Journal of Law & Technology 351

Ruth Janal, 'Data Portability - A Tale of Two Concepts' (2017) Volume 8 JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 59

Ryff CD 'Happiness is everything, or is it? Explorations on the meaning of psychological well-being' [1989] 57 Journal of personality and social psychology 1069.

Santos C Dos and others, 'LAPSI 1.0 Recommendation on Privacy and Data Protection' <http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366>

Savin A, *EU Internet Law* (Edward Elgar 2017)

Schauer FF, *Profiles, Probabilities, and Stereotypes* (Harvard University Press 2006)

Schermer B, 'Risks of Profiling and the Limits of Data Protection Law' in B. Custers et al (eds), *Discrimination & Privacy in the Information Society* (Springer 2013)

Schermer B, Custers B and van der Hof S, 'The Crisis of Consent' [2013] Ethics & Information Technology.

Schneider I, 'Big Data, IP, Data Ownership and Privacy: Conceptualising a Conundrum a Presentation at the 10th Annual Conference of the EPIP Association in Glasgow' (2-3 September 2015) <http://www.epip2015.org/big-data-ip-data-ownership-and-privacy-conceptualising-a-conundrum/>

Schultz J and Perzanowski A, *The End of Ownership; Personal Property in the Digital Economy* (The MIT Press 2016)

Schwartz P, 'Property, Privacy and Personal Data' (2003) 117 Harvard Law Review 2056

Selbst AD and Powles J, 'Meaningful Information and the Right to Explanation' (2018) 7 International Data Privacy Law 233

Shackelford SJ and Russell S, 'Operationalizing Cybersecurity Due Dilligence: A Transatlantic Comparative Case Study' (2017) 67 University of South Carolina Law Review 1

Shmueli G and others, *Data Mining for Business Analytics Concepts, Techniques, and Applications in R* (Wiley 2018)

Skinner E, 'A Guide to Constructs of Control' (1996) 71 Journal of Personality and Social Psychology

549

Smith M, ‘Four German Jurists. II’ (1896) 11 Political Science Quarterly 278

Sokol DD and Comerford R, ‘Antitrust and Regulating Big Data’ [2016] Geo. Mason L. Rev. 1129

Solove DJ, ‘Conceptualizing Privacy’ (2002) 90 California Law Review 1087

——, *The Digital Person* (New York University Press 2004)

——, ‘A Taxonomy of Privacy’ (2006) 154 University of Pennsylvania Law Review 477

Stalla-Bourdillon S and Knight A, ‘Anonymous Data v. Personal Data - a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data’ (2017) 34 Wisconsin International Law Review 285

Stephen C and others, ‘The Internet on Our Terms: How Children and Young People Deliberated About Their Digital Rights’ (2017) <https://casma.wp.horizon.ac.uk/wp-content/uploads/2016/08/Internet-On-Our-Own-Terms.pdf>

Stilman G, ‘The Right to Our Personal Memories: Informational Self-Determination and the Right to Record and Disclose Our Personal Data’ (2015) 25 Journal of Evolution and Technology 14

Stucke ME and Grunes AP, ‘No Mistake About It: The Important Role of - Antitrust in the Era of Big Data’ [2015] University of Tennessee Legal Studies Research Paper

Suzanne Rodway, ‘Just How Fair Will Processing Notices Need to Be under the GDPR?’ (2016) 16 Data Protection - A Practical Guide to UK and EU Law

Swedloff R, ‘Risk Classification’s Big Data (R)evolution’ 21 Conecticut Insurance law Journal 339

Tavani HT, ‘KDD, Data Mining, and the Challenge for Normative Privacy’ (1999) 1 Ethics and Information Technology 265

Taylor L, Floridi L and van der Sloot B (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

Tene O and Polonetsky J, ‘Big Data for All: Privacy and User Control in the Age of Analytics’ (2013) 11 Northwestern Journal of Technology and Intellectual Property 240

Tennison J, ‘Data Portability’ (*Jeni's Musings*, 26 December 2017) <http://www.jenitennison.com/2017/12/26/data-portability.html>

Thomas Wischmeyer, ‘Informationssicherheitsrect: IT-Sicherheitsgesetz Und NIS-Richtlinie Als Elemente Eines Ordnungsrechts Für Die Informationsgesellschaft’ (2017) 50 (2) Die Verwaltung,

Tjong Tjin Tai E, ‘The Right to Be Forgotten - Private Law Enforcement’ (2017) 30 (1-2) International Review of Law, Computers & Technology

Tridimas T, ‘Fundamental Rights, General Principles of EU Law, and the Charter’ (2014) 16 Cambridge Yearbook of European Legal Studies 361

Tsesis A, ‘The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data’ (2014) 49 Wake Forest Law Review 433

Tucker DS and Wellford HB, ‘Big Mistakes Regarding Big Data’ [2014] The Antitrust Source

UK Information Commissioner Office, ‘Subject Access Code of Practice’ <https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf>

——, ‘Guidance on the Rules on Use of Cookies and Similar Technologies’ <https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf>

——, ‘Feedback Request – Profiling and Automated Decision-Making’ <https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>

——, ‘The Guide to Data Protection’ <http://www.inf.ed.ac.uk/teaching/courses/pi/2017_2018/PDFs/guide-to-data-protection-2-9.pdf>

Urquhart L, Sailaja N and McAuley D, ‘Realising the Right to Data Portability for the Domestic Internet of Things’ (June 2017) Personal Ubiquitous Computing

Ursic H, ‘The Right to Be Forgotten or the Duty to Be Remembered? Twitter Data Reuse and Implications for User Privacy’ (2016) <https://bdes.datasociety.net/wp-content/uploads/2016/10/Ursic-politiwoops.pdf>

Ursic H and Custers B, ‘Legal Barriers and Enablers to Big Data Reuse A Critical Assessment of the Challenges for the EU Law’ [2016] 2 European Data Protection Law Review 209

E and International Association of Privacy Professionals, *European Privacy: Law and Practice for Data Protection Professionals* (International Association of Privacy Professionals (IAPP) 2012)

van der Auwermelen B, ‘How to Attribute the Right to Data portabÍlity in Europe: A Comparative Analysis of Legislations’ (2016) 33 Computer Law & Security Review 57

van Der Hof S and Lievens E, ‘The Importance of Privacy by Design and Strengthening Protection of Children ’ S Personal’ (2018) 23 Communications Law

van der Hof S, Schermer B and Custers B, ‘Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies’ (2014) 6 Policy and Internet

van der Sloot B, ‘How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One’ (2015) 24 Information and Communications Technology Law 74

——, ‘Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR’s Case Law on Privacy Violations Arising from Surveillance Activities BT’ in S Gutwirth, R Leenes and P De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy* (Springer 2016)

van Alsenoy B, '*Regulating Data Protection - The Allocation Of Responsibility And Risk Among Actors*

Involved In Personal Data Processing' (PhD Thesis, KU Leuven, 2016)

van Alsenoy B, Verdoot V, Heyman R, Ausloos J and Wauters E, 'From Social Media Service to Advertising Network: a critical analysis of fakebook's revised policies and terms' Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property of KU Leuven and the department of Studies on Media of the Vrije Universiteit Brussel (2015).

van Hoboken J, 'The Proposed Right to Be Forgotten Seen from the Perspective of Our Right to Remember (Prepared for the European Commission)' (2013) <http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo Be Forgotten_Manuscript_2013.pdf>

van Hoboken J, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and Us Frameworks for Personal Data Processing' in B Van Der Sloot, D Broeders and E Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016)

van Middelaar L, *The Passage to Europe: How a Continent Became a Union* (Yale University Press 2013)

Vanberg AD and Ünver MB, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8 European Journal of Law and Technology 1 <http://ejlt.org/article/view/546>

Vayena E and Gasser U, 'Between Openness and Privacy in Genomics' (2016) 13 PLoS Medicine 1

Veale M, Binns R and Ausloos J, 'When Data Protection by Design and Data Subject Rights Clash' (2018) forthcoming in International Data Privacy Law

Veale M, Binns R and Edwards, L, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law (2018)' 376 Philosophical Transactions of the Royal Society

Veale M and Edwards L, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398

Victor JM, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 The Yale Law Journal 513

Vissers T and others, 'Crying Wolf ? On the Price Discrimination of Online Airline Tickets' (2014) <https://hal.inria.fr/hal-01081034/document>

Voss G and Castets-Renard C, 'Proposal for an International Taxonomy on the Various Forms of the "Right To Be Forgotten": A Study on the Convergence of Norms' (2016) 14 Colorado Technology Law Journal 281

Vries K De, Depreeuw S and Hildebrandt M, 'D3.2 Profile Transparency, Trade Secrets and Intellectual Property Rights in OSNs – v1 (Deliverable for the USEMP Project)' (2015) <http://www.usemp-project.eu/wp-content/uploads/2015/05/usemp_deliverable_d3.2_revised.pdf>

Wachter S, ‘Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR’ [2017] 34 (3) Computer Law & Security Review

Wachter S, Mittelstadt B and Floridi L, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ [2017] 7 (2) International Data Privacy Law

Wachter S, Mittelstadt B and Russell C, ‘Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR’ (2018) 31 Harvard Journal of Law & Technology 2

Walker K, ‘Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange’ (2000) 190 Stanford Technology Law Review 1

Wang Y and Shah A, ‘Supporting Data Portability in the Cloud Under the GDPR’ <http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf>

Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193

Watson P and Ellis E, *EU Anti-Discrimination Law* (Oxford University Press 2012)

Weiss GM and others, ‘Smartwatch-Based Activity Recognition: A Machine Learning Approach’, *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (2016) <http://storm.cis.fordham.edu/gweiss/papers/bhi-ar-2016.pdf>

Werro F, ‘The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash’ in Aurelia Colombi Ciacchi and others (eds), *Haftungsbereich im dritten Millennium / Liability in the Third Millennium* (Nomos 2009)

Wessel RA, ‘Towards EU Cybersecurity Law: Regulating a New Policy Field’ in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

Westin AF, *Privacy and Freedom* (Ig Publishing 2015)

Westin AF, ‘Social and Political Dimensions of Privacy’ (2003) 59 Journal of Social Issues 431 <https://doi.org/10.1111/1540-4560.00072>

Whish R and Bailey D, *Competition Law* (Oxford University Press 2012)

Whittington J and Hoofnagle CJ, ‘Unpacking Privacy’s Price’ (2012) 90 North Carolina Law Review

Xue M and others, ‘The Right to Be Forgotten in the Media: A Data-Driven Study’ (2016) 4 Proceedings on Privacy Enhancing Technologies <https://petsymposium.org/2016/files/papers/The_Right_to_be_Forgotten_in_the_Media__A_Data-Driven_Study.pdf>

Zanfir G, ‘The Right to Data Portability in the Context of the EU Data Protection Reform’ (2012) 6 International Data Privacy Law

——, ‘Drepturile Persoanei Vizate În Contextul Prelucrării Datelor Private’ (PhD Thesis, University of Craiova 2013)

Zarsky TZ, '"Mine Your Own Business!": Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion' (2002) 5 Yale Journal of Law and Technology 1306

——, 'Incompatible: The GDPR in the Age of Big Data' (2018) 94 Seton Hall Law Review 995

Zech H, 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 Journal of Intellectual Property Law & Practice 460

Zhe Jin G, 'Artificial Intelligence and Consumer Privacy' (2017) <http://www.nber.org/chapters/c14034>

Zifcak S, *Globalisation and the Rule of Law* (Routledge, London; New York, 2005)

Zuboff S, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75 <http://dx.doi.org/10.1057/jit.2015.5>

Zuiderveen Borgesius FJ, 'Improving Privacy Protection in the Area of Behavioural Targeting' (PhD Thesis, University of Amsterdam 2014)

——, 'Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 Computer Law & Security Review

——, 'Should We Worry about Filter Bubbles?' (2016) 5 Internet Policy Review 1

Zuiderveen Borgesius FJ and others, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (2017) <https://www.ivir.nl/publicaties/download/IPOL_STU2017583152_EN.pdf> accessed 17 November 2017

Zuiderveen Borgesius FJ and Poort J, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347

Zwenne G-J, 'Diluted Privacy Law' (2013) <https://zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-Diluted-Privacy-Law-inaugural-lecture-Leiden-12-April-2013-ENG.pdf>

Curriculum Vitae

Helena U Vrabec works for Palantir (US) and is part of the privacy and legal teams.

Since January 2018 to June 2018 Helena was a resident fellow at Yale ISP. Before coming to Yale, she worked 3 years as a researcher and PhD candidate at Leiden Law School (the Netherlands). During the years in Leiden she was also a European Commission ethics expert, and gave lectures on privacy law for students and legal professionals. Prior to that, she worked as a privacy advisor for Ernst & Young in Amsterdam. Helena previously taught business law at the University of Ljubljana, School of Business (Slovenia), and was a trainee at the Slovenian Embassy in Austria.

Helena regularly publishes in peer-reviewed journals on the topics in relation to data protection, big data and law & technology, and gives talks at national and international conferences. For her academic achievements, she was awarded several academic grants and awards, among others the Fulbright and the Meijers prize.

Helena holds a master's degree in law from Ljubljana University (2013) and an LLM from Tilburg University (2014).

Acknowledgements

In many ways, 'Uncontrollable: Data Subject Rights in the Data-Driven Economy' is a metaphor for my PhD years during which I had the privilege to undergo, just like the EU data protection law, a true and thourough metamorphosis. I started my research in an era of an unprecedented data-driven revolution and was quickly soaked up in the fast-paced environment where I could not restrict myself to the role of a passive observer. It was an exciting time for a PhD student who had learnt only five years ago that data protection law existed. Today, I am proud to continue my mission as a data protection lawyer for one of the world's most innovative data-driven companies.

At this point I would like to thank Bart and Simone for being extremely supportive, understanding but also demanding and detail-oriented mentors. Bart, working with you was inspiring and motivating. Thanks for giving me some of the most valuable academic advice and truly leading by example. Simone, I always felt privileged to be mentored by you not only because of your great expertise of the field, but also because of the ability to stand by your principles and to lead with humbleness.

The eLaw family – thank you for creating a warm and inspiring environment in which my research started and grew. Jenneke and Tobias – thank you for being the best paranyphen. I could not do it without you! Thank you, the EUDECO team, for the lively discussions and optimistic handling of the challenging EC H2020 project which formed a basis for my further doctoral reearch. Thank you, Nora, Emilia, Swati and the rest of the former EY dream team, for drawing me into the privacy world and reminding me of how powerful women can be.

The time I spent as a resident fellow at Yale ISP was a cherry on top of my PhD cake. I remain indebted to Jack Balkin, Rebecca Crootof and the whole ISP family for giving me the opportunity to benefit from the intelectually stimulating environment at Yale and to interact with some of the brightest people I had met, and to Leids Universitair Fonds for the financial support.

Finally, thank you the PCL team and the ninjas for your warm welcome and for giving me the opportunity to apply my knowledge in practice, where it is, I strongly believe, most needed. I look forward to upcoming adventures at Palantir.

Outside the professional world, my PhD years would not be the same without the friends that I met in the Netherlands and elsewhere, in particular my closest VTIS family – Aleksandra, Anton and Timotej. During my quick and always rushed trips to Slovenia, coffee chats with Ana T., Tomaž, Neža, Katja, Ana U. and Maruša were special and energizing, and I am gratful for the efforts you have been putting into keeping our friendship alive despite the distance.

Finally, I would like to say thanks to my dear (extended) family for keeping me in their prayers (nona Milka!) and thoughts. Thank you, Ana and Tadej U., for always being available for remote emergencies and help. Thank you, mum and dad, for encouraging me to love books and science ever since I was a little girl. And last but not least, thank you, Tadej V., for tirelessly listening to my academic monologues, for motivating me to dream and dare, and for being my safe harbour and my best friend.