Uncontrollable: Data subject rights and the data-driven economy

Ursic, H.

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

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.