Shattering one-way mirrors – data subject access rights in practice

Jef Ausloos* and Pierre Dewitte*

Key Points

- The right of access occupies a central role in EU data protection law's arsenal of data subject empowerment measures. It can be seen as a necessary enabler for most other data subject rights as well as an important role in monitoring operations and (en)forcing compliance.
- Despite some high-profile revelations regarding unsavoury data processing practices over the past few years, access rights still appear to be underused and not properly accommodated. It is especially this last hypothesis we tried to investigate and substantiate through a legal empirical study.
- During the first half of 2017, around 60 information society service providers were contacted with data subject access requests. Eventually, the study confirmed the general suspicion that access rights are by and large not adequately accommodated. The systematic approach did allow for a more granular identification of key issues and broader problematic trends. Notably, it uncovered an often-flagrant lack of awareness; organization; motivation; and harmonization.
- Despite the poor results of the empirical study, we still believe there to be an important role for data subject empowerment tools in a hyper-complex, automated, and ubiquitous data-processing ecosystem. Even if only used marginally, they provide a checks and balances infrastructure overseeing controllers' processing operations, both on an individual basis as well as collectively. The empirical findings also allow identifying concrete suggestions aimed at controllers, such as relatively easy fixes in privacy policies and access rights templates.

Introduction

EU data protection law offers individuals an arsenal of rights they can exercise against controllers. Among them, the right of access constitutes a cornerstone of data subjects' informational empowerment. The right allows individuals to monitor what personal data are held about them, how it is being processed and with whom it is shared. Especially in light of a growingly complex data processing eco-system and the increased reliance on 'data' to make all kinds of (life-affecting) decisions, the right of access can play a crucial role in safeguarding fairness, accountability, and responsibility. All the more considering the one-way mirrors many controllers have erected around them. Indeed, the right of access offers an effective opportunity to break through information asymmetries so prevalent in the context of information society services today.

In practice, however, the right of access—and data subject rights more broadly—is/are often said to be ignored, inefficient, underused and/or obsolete. Nevertheless, not much empirical research exists actually substantiating these claims. Anecdotal evidence does suggest some truth to the former three allegations,[1] but concluding therefore

* Jef Ausloos and Pierre Dewitte, CiTiP (Centre for IT and IP Law), KU Leuven, Leuven, Belgium. The authors would like to thank the many individuals who have made this article possible, in particular Louise Flamey and Pinelopi Servata who helped gathering the empirical data, Rob Heyman (VUB—SMIT—imec) who co-developed the methodology for conducting the empirical research underlying this article and Paul-Olivier Dehaye (PersonalData.io) for providing the infrastructure to gather empirical data as well as enlightening us with many real-life examples and insights drawn from his own experience. The authors report no declarations of interest.

1 Zeit Online, 'Verräterisches Handy' *Zeit Online* (February 2011) <https://web.archive.org/web/20180110212132/http://www.zeit.de/datenschutz/malte-spitz-data-retention> accessed 8 February 2018; Cyrus Farivar, 'How One Law Student Is Making Facebook Get Serious about Privacy' (*Ars Technica*, 15 November 2012) <https://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/> accessed 8 February 2018; Judith Duportail, 'I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets' *The Guardian* (26 September 2017) <http://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold> accessed 8 February 2018. Due credit should be given to

that (some) data subject rights are obsolete seems unwarranted. In order to have an informed debate—grounded in practical reality—we set out to gather empirical data on how data subject rights are exercised and accommodated in the field. While the initial focus was on the rights of access and erasure, only limited information was gathered on the latter. This article therefore focuses on the right of access only. Nonetheless, it is deemed that the findings are already quite useful in demonstrating systematic issues regarding the accommodation of data subject rights more broadly. While the empirical findings do indeed confirm some suspicions (eg underused, ignored), they allow to pinpoint key obstacles much more precisely and therefore facilitate devising ways on how to overcome these obstacles.

In sum, it is this article's ambition to provide the necessary evidence for having a fully informed debate on the practical issues relating to the right of access. In order to do so, the Section 'The present. Empirically testing access right compliance' will first run the reader through the right of access' historical context. This will enable a proper understanding of the current status quo as described in the Section 'The future. A new era for data subject rights?', which illuminates the findings of the empirical study. The Section 'Conclusion', finally, looks ahead and attempts at drawing broader conclusions as to the future of data subject rights, as well as making cautious recommendations on how to overcome the issues identified in the Section 'The future. A new era for data subject rights?'. In short, we hope the article contributes to the broader debate on how to align and ensure principles such as fairness, responsibility, and accountability in the data processing ecosystem trickle down to practical reality.

The past. Tracing access rights' contours

Historical roots

History. The right of access has always been integral to data protection.[2] The Council of Europe included it as a sixth principle in its 1973 Resolution, explaining that a right to have access—including information on the nature of the data, the actual data, and how that data is used—can be considered 'an essential minimum element in the protection of privacy'.[3] Indeed, across the Atlantic in the 1960s already, academics[4] and policymakers[5] were discussing the contours of individual access to data as an important safeguard against the backdrop of burgeoning large-scale automated data processing. Both in Europe and the US, different conceptualizations of the right of access were formulated, ranging from a general right to know that data is being processed, to a much more detailed 'right to a print-out' (ie a right to automatically receive all one's information at regular intervals).[6] Yet, the most widely accepted form of 'access' across pioneering data protection Member States in the EU was 'the right to be informed on request'.[7]

From obligation to right. Despite the right of access being an item in data protection policy-making for over half a century already, it should be said that in 'first generation' frameworks, it was primarily data protection commissioners (or their functional equivalents) who were expected to enforce the rules.[8] In other words, empowering individuals to exert their data protection interests was not a policy goal throughout most of the 1970s.[9] Gradually though, the primarily 'protective' approach to data protection of the first generation was complemented by empowerment measures in the second generation towards the late 1970s.[10] Individuals

one large-scale academic study investigating the right of access in practice across the EU: Clive Norris and others, *The Unaccountable State of Surveillance* (Springer International Publishing, Cham, Switzerland 2017). This book constitutes the 5th work package of the IRISS project; details available at the address: <www.irissproject.eu>.

2 Yet not universally incorporated in the first data protection legislations. See individual country reports in: Frits W Hondius, *Emerging Data Protection in Europe* (Amsterdam: North-Holland 1975).

3 Explanatory Report to: Council of Europe–Committee of Ministers, 'Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-À-Vis Electronic Data Banks in the Private Sector' para 30. A year later, a similar principle was also included in: Council of Europe–Committee of Ministers, 'Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector'.

4 Kenneth L Karst, '"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data' (1966) 31 Law and Contemporary Problems 342; Arthur R Miller, 'Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society' [1969] Michigan Law Review 1089.

5 Caspar Weinberger, *Records, Computers and the Rights of Citizens* (US Department of Health, Education and Welfare, Washington DC 1973).

6 Though the latter did not receive much support at the time, it was later incorporated into the Council of Europe's Convention 108. Miller (n 4) 1212 Referring to senate hearings and other doctrinal sources, including; Alan F Westin, *Privacy and Freedom* (Ig Publishing, New York 1967); Hondius (n 2) 152–57.

7 Hondius (n 2) 152–57.

8 Viktor Mayer-Schönberger, 'Generational Development of Data Protection In Europe' in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (First, MIT Press 1998) 221–25.

9 Ibid.

10 Which can be situated in French, Austrian, Danish, and Norwegian legislation. Ibid 226–29.

were given a more prominent role through specific data protection *rights*, with the right of access constituting the first meaningful *ex post* empowerment measure.[11] As a matter of fact, up until Directive 95/46,[12] the right was actually seen as a central provision encapsulating other key rights such as the right to correct and erasure.[13]

International stage. The 1980 OECD Guidelines on privacy marked the first occurrence of the right of access in an international statement extending beyond Europe.[14] Included in the 'Individual Participation Principle', this right of access was limited to confirmation of whether data is being processed and the actual data itself. Despite this limited scope, the principle does lay down important requirements that still prove crucial today: (i) communication needs to occur with a reasonable time; (ii) at no (excessive) charge; (iii) in a reasonable manner; and (iv) in a readily intelligible form. A year later, the Council of Europe's Convention 108 included a similar right, adding the ability to get access to the main purposes of processing, the identity and location of the controller and, interestingly, the right to receive one's personal data at regular intervals.[15]

Fundamental rights dimension. Today, the right of access also has a fundamental rights dimension. Progressively, the extensive interpretation suggested by the ECtHR has included a right of access into the scope of Article 8 ECHR.[16] Indeed, the Strasbourg Court has already stressed that denying or ignoring an access request, whether in the case of information held by public authorities or private actors, could amount to a disproportionate interference under Article 8, section 2 of the ECHR if that decision failed to strike a fair balance between competing interests.[17] In 2009, the entry into force of the 2000 Charter of Fundamental Rights of the European Union[18] has officially granted the protection of personal data the status of a EU fundamental right.[19] With Article 8, section 2 of the Charter explicitly referring to the right of access, this right has been confirmed as one of the data subjects' most significant tools designed to guarantee the effective protection of their personal data.

Data protection directive. Adopted in the mid-nineties, Article 12(a) Directive 95/46 aimed to harmonize the right of access in secondary law across Member States. The provision grants data subjects the right to obtain confirmation from controllers as to whether or not personal data concerning them is being processed and, where that is the case, access to several categories of information.[20] Unsurprisingly, the right of access hinges upon the definition of 'personal data', a highly contentious and dynamic concept itself.[21] From a procedural

11 '*Ex post*' referring to the fact that these are data subject rights which only become applicable *after* processing operations have initiated. Mayer-Schönberger acknowledges that such a right was already present in the first generation of data protection norms. He explains, however, that in these first frameworks, the right to access and correct was merely there to support 'accuracy requirements'. Mayer-Schönberger (n 8) 226–27. Also see: Hondius (n 2) 112–15; Herbert Burkert, 'Privacy-Data Protection: A German/European Perspective', *2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council* 45 <http://www.coll.mpg.de/sites/www/files/text/burkert.pdf> accessed 8 February 2018; Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, Ithaca 1992) 103-106-158.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [1995] OJ L281/31.

13 See *inter alia*: Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff, Leiden 2013) 29.

14 Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, 23 September 1980. More specifically, part two of these guidelines contains the 'individual participation principle' which in turn advocates for the granting of a right to access. For an account of the coming into being of the 1980 OECD guidelines on privacy, see: Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 International Data Privacy Law 6.

15 Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 28th January 1981. See Article 8*b* of the Convention 108 whose wording is very similar to the 'individual participation principle' introduced by the OECD guidelines. It is worth noting that this Convention is currently under revision; on that point, see: Cécile De Terwangne, 'The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data' (2014) 28 International Review of Law, Computers & Technology 118–130.

16 For more information about data protection as a fundamental right under the case law of the ECtHR, see: Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing, Cham, Switzerland 2014), especially ch 4, point 4.3, 94–103; Päivi Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (2013) 5 Journal of Media Law 79–103; Gordon Nardell QC, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Netherlands: Springer 2010) 43–52.

17 See ao: ECtHR, *Leander v. Sweden*, 26 March 1987; *Gaskin v. the United Kingdom*, 7 July 1989; *Z v Finland*, 25 February 1997; *MG v the United Kingdom*, 24 December 2002; *Odièvre v France*, 13 February 2003; *I v Finland*, 17 July 2008; *Haralambie v Romania*, 27 October 2009.

18 Charter of Fundamental Rights of the European Union, *OJEU*, 2000, C 364/1.

19 For a detailed analysis of the drafting and scope of the CFREU, see: Fuster (n 16) 192–205.

20 The right of access has consequently been qualified as a 'two-steps approach': Raphaël Gellert and Serge Gutwirth, 'Citizens Access to Information: The Data Subject's Rights of Access and Information: a Controllers' Perspective' in *Privacy, Data Protection and Ethical Issues in New and Emerging Technologies: Assessing Citizens' Concerns and Knowledge of Stored Personal Data*, Deliverable 3 of the PRESCIENT Project, 15 May 2012.

21 See notably the CJEU's recent case law (eg *Peter Nowak v Data Protection Commissioner*, Case C-434/16 (ECLI:EU:C:2017:994); *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14 (ECLI:EU:C:2016:930).

perspective, however, the relative absence of any practical requirements within Directive 95/46 has resulted in Member States all developing their own set of modalities for exercising the right of access.[22] These modalities and the corresponding position of relevant actors (ie data subjects, controllers and processors) have further been shaped by national DPAs and domestic case law.[23] As a result, there are currently no straightforward European-wide legal prescriptions governing the practical application of the right of access, but rather a patchwork of national traditions and legislations. Neither the CJEU, nor the Article 29 Working Party (WP29) has tackled this fragmentation on modalities for exercising the right of access.[24]

Unknown, unloved?

Conceptually speaking, the right of access appears as a cornerstone of data subjects' informational empowerment.[25] The right allows data subjects to learn what personal data are held about them, how they are being processed and with whom they are or may be shared.[26] As such, it lies at the heart of EU data protection law and indeed the realization of the fundamental right to data protection's (Article 8 Charter) 'control rationale'. The right of access both acts as a necessary first step enabling the exercise of most other data subject rights, and as a strategic tool to assess compliance with data protection law more broadly. Despite these important functions, the right still seems underused and underappreciated in practice.

Sine qua non. First and foremost, the right of access constitutes an essential first step toward the exercise of other prerogatives granted to data subjects (*Chapter III – Rights of the Data Subjects* in the GDPR). Neither rectification or erasure of personal data, nor blocking or objecting to the processing of personal data seem easy or even possible unless the data subject knows exactly what data the controller processes and how.[27] In light of this, the right of access has already been qualified as the 'natural precondition' [28] for data subjects to exercise their remaining informational rights.[29] The positioning of the right of access within Article 12 Directive 95/46 which also encompasses the right to rectification, erasure and blocking in its point (b) is, in that sense, far from being a mere coincidence (above). Neither is the fact that access heads the list of rights provided for in the General Data Protection Regulation.[30] The right of access' pivotal role has also been confirmed by the CJEU in *College van burgemeester en wethouders van Rotterdam*, where it stated that the '*right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) [. . .] Article 14 of the Directive [. . .] or his right of action where he suffers damage, laid down in Articles 22 and 23 thereof*'.[31] More

22 In Belgium, the Directive has been transposed by the Privacy Act of 8 December 1992 (Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, *Belgian Official Journal*, 18 March 1993, p 5801) and completed by the Royal Decree of 13 February 2001 (Royal Decree implementing the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, *Belgian official Journal*, 13 March 2001, p 7839). The Belgian law stipulates, for example, that an access request should be dated and signed (Art 10, s 1, al 2), answered within the 45 days following the request (Art 10, s 1, al 3), and that data subjects may be requested to prove their identity (Art 10, s 1, al 1). It should also be free of charge.

23 For a comprehensive overview of the Member States' different legislative frameworks, see: Antonella Galetta and others, 'Mapping the Legal and Administrative Frameworks of Informational Rights in Europe – A Cross-European Comparative Analysis' in Clive Norris and others (eds), *The Unaccountable State of Surveillance* (Springer International Publishing, Cham, Switzerland 2017) ch 15, point 15.3 (for legislative peculiarities) and 15.4 (for an overview of relevant case law) 459–71.

24 The CJEU only dealt with the 1-year time limit set up by the Dutch transposing act for the exercise of the rights of access. Having struck a balance between the competing interests of data subjects to obtain access to their data on the one hand, and of controllers not to undergo excessive retention obligation on the other hand, the CJEU held that such a short period did '*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*' (*College van burgemeester en wethouders v MEE Rijkeboer*, Case C-553/07 (ECLI:EU:C:2009:293), para 66. See also on that specific point: Jean-Marc Van Ghyseghem, and others, 'La protection des données à caractère personnel en droit européen' (2014) 1 Journal Européen des Droits de l'Homme 69. It is worth noting that the pronouncements of the ECtHR dealing with the right of access are quite irrelevant when it comes to circumscribing the modalities of the right of access as all the cases referred to in note 17 merely deal with the question of whether or not denying an access request constitutes a justified interference according to art 8.2 ECHR. Nevertheless, the ECtHR has repeatedly emphasized the importance of instituting independent and impartial bodies that are vested with the competence to make judgments on the right of access. See note 23, point 15.4.

25 Steven Lorber, 'Data Protection and Subject Access Request' (2004) 33 Industrial Law Journal 180; Xavier L'Hoiry, Clive Norris, 'Introduction – The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (eds), *The Unaccountable State of Surveillance*, (Springer International Publishing 2017) 1-8.

26 At least in the GDPR. Directive 95/46 only granted data subjects the possibility to ask for whom the data had been shared with already.

27 As a matter of fact, data subjects can ask for their data to be erased without first having to request access to them. Doing so may render it difficult however, to evaluate whether one's request is adequately accommodated.

28 Xavier Duncan L'Hoiry and Clive Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 International Data Privacy Law 190.

29 Sometimes jointly referred to as ARCO rights (ie access, rectification, cancellation, opposition). See: ibid 190; Antonella Galetta and Paul de Hert, 'A European Perspective on Data Protection and the Right of Access' in Clive Norris and others (eds), *The Unaccountable State of Surveillance* (Springer International Publishing, Cham, Switzerland 2017) 25.

30 Regulation 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 L119/1.

31 *College van burgemeester en wethouders v MEE Rijkeboer* (n 24), ss 51–52.

recently, the link between the right of access and the effective exercise of other prerogatives has been underlined in the WP29's guidelines on data portability.[32] Similarly, in her opinion in *Peter Nowak v Data Protection Commissioner*, Advocate General Kokott emphasized that the right of access effectively appears a logical path to rectification.[33]

A tool to monitor controllers' compliance with data protection rules. Second, the right of access allows data subjects to monitor controllers' compliance with the general principles governing the processing of personal data, notably Articles 5–6 GDPR (Articles 6–7 Directive 95/46). Especially compliance with the purpose limitation, data minimization, accuracy, and storage limitation principles[34] should be relatively easily verifiable after obtaining access. In the same vein, compliance with privacy policies can also be assessed by comparing the agreed terms and conditions with their effective application by the controller. This can prove useful, particularly when it comes to assessing the (continued) lawfulness of processing pursuant to Article 6(1) of the GDPR (Article 7 Directive 95/46), as well as monitoring the recipients to whom personal data may have been transmitted by the original controller. This monitoring role of the right of access has also been recognized by both Directive 95/46 and the GDPR.[35] If the exercise of the right lays bare violations, it goes without saying that data subjects are entitled to take action either by approaching controllers directly and/or by seeking remedies before DPAs or national courts.[36] Max Schrems' actions against Facebook provide the best illustration of the effectiveness of this remedial function. After a lecture by a Facebook representative during a study-exchange at Santa Clara University, California, Schrems filed an access request with the company. He received an enormous PDF file (including previously erased data) and initiated proceedings before the Irish DPA.[37] In doing so, he was one of the first successful trailblazers for shedding light on Facebook's breaches of European data protection rules[38] and through his actions brought the CJEU to declare the Commission's Safe Harbour decision invalid.[39] All of this, starting from Facebook's response to one Austrian law student's access request. In that sense, the right of access does not only consist of an essential first step in exercising other data subject rights, but also turns out to be crucial in assessing controllers' compliance with general principles as well as initiating remedial and enforcement actions.

Lost potential. Despite the above, the right of access' potential prowess for contributing to data subjects' empowerment and monitoring controllers' compliance, remains rather latent. Practical reality suggests that it has not gained substantial popularity among data subjects.[40] Looking at the other side, controllers themselves seem to struggle with its practical implementation as well (cf. following section). Several field studies reporting on the issues related to exercising data subjects' informational rights in a variety of situations have not (yet) caused much change in the attitudes of either controllers or data subjects.[41] Having said that, in the pst

32 Art 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, WP242. See p 4, where the WP29 explicitly states that the right of data portability '*complements the right of access*'. Indeed, the real problem faced by data subjects when requesting access to their data under Directive 95/46 is to be '*constraint by the format chosen by the data controller to provide the requested information*' (p 3). Therefore, data portability brings precision as to the format in which information should be provided.

33 Opinion of Advocate General Kokott delivered on 20 July 2017 in *Peter Nowak v Data Protection Commissioner* (n 21) especially point (b): 'Rectification of data', ss 35–41.

34 Arts 5(1)b, c, d and e of the GDPR (Arts 6(1)b c d and e Directive 95/46).

35 Recital 63 of the GDPR emphasises that '*a data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing*'. A similar idea was already laid down in Recital 41 Directive 95/46.

36 On the links between the right of access to personal data and the right to an (effective) remedy for data protection violations, see: Antonella Galetta and Paul de Hert, 'The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?' (2015) 8 Review of European and Administrative Law 125–51.

37 On the proceedings before the Irish DPA and the CJEU, see: Steve Peers, 'The Party's Over: EU Data Protection Law after the Schrems Safe Harbour Judgment' *EU Law Analysis* (7 October 2015) <https://eulawanalysis.blogspot.be/2015/10/the-partys-over-eu-data-protection-law.html> accessed 8 February 2018; Electronic Privacy Information Centre, 'Schrems v Data Protection Commissioner' <https://epic.org/privacy/intl/schrems/> accessed 8 February 2018.

38 Meanwhile, several data protection authorities have also started proceedings against the social network, with varying degrees of success. See: Cara McGoogan, 'Facebook Hit with €1.2m Fine in Spain for Breaking Privacy Laws' *The Telegraph* (11 September 2017) <http://www.telegraph.co.uk/technology/2017/09/11/facebook-hit-12m-fine-spain-breaking-privacy-laws/> accessed 8 February 2018.

39 *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14 (ECLI:EU:C:2015:650).

40 This also appears from some of the answers received in the empirical research explained below, where several online service providers either expressly stated or implied that they are almost never confronted with data subjects exercising their rights.

41 See references in note 1. See also, for a practical analysis of the right of access in the European countries, see: Norris and others (n 1). For a study on the right of access in Italy and Belgium, see: Antonella Galetta, Chiara Fonio and Alessia Ceresa, 'Nothing is as it Seems. The Exercise of Access Rights in Italy and Belgium: Dispelling Fallacies in the Legal Reasoning from the "law in theory" to the "law in practice"' (2016) 6 International Data Privacy Law 16–37. For an undercover field study on the effectivity of the right to erasure among popular smartphone apps and websites in Germany, see: Dominik Herrmann and Jens Lindemann, 'Obtaining Personal Data and Asking for Erasure: Do App Vendors and Website Owners Honour your Privacy Rights?' <https://arxiv.org/abs/1602.01804> accessed 8 February 2018). For a study covering the exercise of the right of access in the context of CCTV in the UK, see: Keith Spiller, 'Experiences of

few years there has been a growing number of (and apparent interest in) tools and platforms facilitating the drafting, follow-up and assessment of access requests.[42] Still, for the time being these empirical studies and tools facilitating the exercise of data subject rights seem rather marginal. Given their importance to both policymakers (eg drafting codes of conduct) and the public at large (eg raising awareness), we still see an important role in the further development and expansion of such efforts. It is against this backdrop that we decided to conduct further empirical research to nurture the discussion on data protection and ensure a more efficient *and* effective application of the law across the board.

The present. Empirically testing access right compliance

Methodology

Despite the ample data protection policy discourse over the past six years, data on actual compliance rates with data subject rights *in the field* are rather scarce.[43] Combined with the overall disparity and uncertainty on the *modus operandi* of the right of access, we set out to gather empirical evidence on compliance with the right of access in the sector of consumer-facing online service providers.

General set-up. After a preparatory phase, the actual collection of information took place between February 2017 and July 2017. Three students following an advanced master's programme (in IT & IP Law) at the KU Leuven,[44] were recruited to participate in this research as part of their thesis-writing project. In deliberation with these students, a selection of 66 commonly used (across the EU) information society service providers was made.[45] These were spread across the following sectors: sharing economy (22 per cent); social media (26 per cent); eCommerce (22 per cent); user generated content (UGC) platforms (12 per cent); email providers (6 per cent); online publishers (5 per cent); online hosting and file storage (3 per cent); Internet of Things (IoT) services (3 per cent); online games (1 per cent).[46] Despite many service providers being active in several of these sectors simultaneously, they were each only categorized into one, according to their core functionality to end-users. The unequal spread can be explained by different market constellations in each of these sectors. It was also decided to leave the selection to the students, so as to best represent the main services they frequently use. We therefore consider the selection to be indicative of the broader landscape and as such adequate for the purposes of this explorative study. Having said that, it is also acknowledged that the modest nature of the list should (and will) be further enriched in the future, ensuring a wider spread.

Information gathering. The list of service providers was equally distributed among the three students who each had to go through the following three steps: (i) register with the service, analyse their privacy policy and perform basic interactions with the service in order to generate user-data; (ii) file an access request; and (iii) actively follow-up and analyse the correspondence with service providers.[47] The findings were gathered through online surveys which the students had to fill in after completing each step for every single service provider. These surveys contained both quantitative (eg how many clicks to find access request instructions, how many days until a reply?) and qualitative (eg how satisfied are you with the process of filing the access request and why?). Even if some answers can be considered subjective (eg using a 1–5 Likert scale to rate the ease of filing one's access request), they still serve as useful indicators. All the more, taking into account the fact that they were provided by advanced master in law

Accessing CCTV Data: The Urban Topologies of Subject Access Requests' (2016) 53 Urban Studies 2885–900. CitizenLab, based at the University of Toronto, has also done a number of studies aimed at shedding light on how personal data is processed (both by corporations and state agencies), see: <https://citizenlab.ca/category/research/transparency/>accessed 8 February 2018. The Access My Information (AMI) platform, is one of the tools developed by CitizenLab.

42 For instance, the following web portals help data subjects to file access requests according to data protection rules: Access My Info (AMI) (<www.accessmyinfo.org>), Bits of Freedom (<www.pim.bof.nl>), PersonalData.IO (<www.personaldata.io>). Other portals are designed to help citizens exercise their freedom of information rights against public authorities and governmental bodies: Alaveteli (<www.alaveteli.org>), AsktheEU (<www.asktheeu.org>), FragDenStaat (<www.fragdenstaat.de>), LobbyPlag (<www.lobbyplag.eu>), MuckRock (<www.muckrock.com>), Transparencia (<www.transparencia.be>), WhatDoTheyKnow (<www.whatdotheyknow.com>). See also the open source Python-based platform Froide designed to run freedom of information websites.

43 Looking at the right of access in particular, one very elaborate study deserves attention: Norris and others (n 1). For a study on the right of access in Italy and Belgium, see: Galetta, Fonio and Ceresa, (n 41). For an undercover field study on the effectivity of the right to erasure among popular smartphone apps and websites in Germany, see: Herrmann and Lindemann (n 42). For a study covering the exercise of the right of access in the context of CCTV in the UK, see: Spiller (n 41).

44 Organised by KU Leuven Centre for IT & IP Law (CiTiP): http://www.law.kuleuven.be/brussel/en/education/intellectual_property_rights/intellectual_property_rights

45 Information Society Service Providers as defined in art 2(a) Directive 2000/31/EC *j.* Directive 98/34/EC and Directive 98/48/EC. Also referred to as 'online service providers' throughout this article.

46 In light of the constant metamorphosis of many online service providers and relevant sectors, it was decided to base this categorisation on examples rather than strict definitions.

47 The empirical research also involved a second phase, where the right to erasure was empirically tested. These findings will not be discussed in this article however.

students that are arguably much more knowledgeable and motivated than the average data subject wishing to exercise data subject rights. Moreover, the students were asked to clarify their answers so that subjective findings were generally also further substantiated by other quantifiable factors (eg number of clicks to get to access request, word-count of privacy policy). Regular meetings between instructor and students (on average >2 times a month) ensured proper follow-up and completion of the surveys. The next section describes the key findings in chronological order and refers to the figures where relevant.

Limitations. Before moving on, two constraints of the study need to be acknowledged. A first important limitation is that it only focuses on desktop websites, even when assessing service providers that are primarily mobile-oriented. It is fair to assume that results may differ—for better or worse—depending on the interface through which one exercises their data subject rights. Secondly, the study was conducted a year before the GDPR's entry into force. The results were therefore assessed with Directive 95/46 as main reference framework. Yet, in order to ensure clarity in the present limbo between two regulatory frameworks, the following pages do refer to both (Directive 95/46 as benchmark for the empirical study and the GDPR between brackets). Section 4 will look more closely at how the evaluation might change once the GDPR enters into force in May 2018.

Ambition. Overall, the goal of this explorative empirical research was to define and test an effective methodology for gathering evidence on compliance with data subject rights. As such, we aim to further develop this methodology and assess different rights (notably the right to erasure, explanation, data portability) in different sectors. We believe that working with (master) students in relevant fields (notably law) makes the research scalable and of high-quality, not to mention that it also offers great educational value. In light of all this, we wish to once again recognize the limited scope of this particular study and invite interested readers to contact us with inquiries on the findings and/or how to incorporate the methodology into their course programmes.

Results

Privacy policy

Accessibility. The very first step towards exercising the right of access is to identify and locate the relevant controller (ie to whom requests must be sent). Since the empirical study strictly focussed on information society service providers (Fig. 1), this was done by browsing their respective websites on a desktop computer[48] and going through their privacy policies.[49] While a vast majority (80 per cent) of investigated privacy policies were reached in only one or two clicks from the homepage (Fig. 2), the process was still rated 'difficult' to 'very difficult' in 31 per cent of instances (Fig. 3).The most important reason in those 31 per cent were poor design, eg by not following today's widespread standard of placing a hyperlink to the privacy section at the bottom of every page. In some cases, information relating to privacy and data protection were also lumped together with the provider's general terms and conditions. In other cases, they were hidden behind a vaguely or wrongly-titled link such as 'Legal terms' or 'Cookies policy'. Important disparities were also observed in the accessibility of privacy policies depending on the main interface used for using the service. Even though the research did not focus on these dissimilarities, it was clear that users might find it easier/harder to find privacy policies depending on whether they are using the service provider's desktop website, a mobile-friendly version of that website or a smartphone app for example. Still, in almost two thirds (64 per cent), the privacy policy was deemed (very) easy to find.

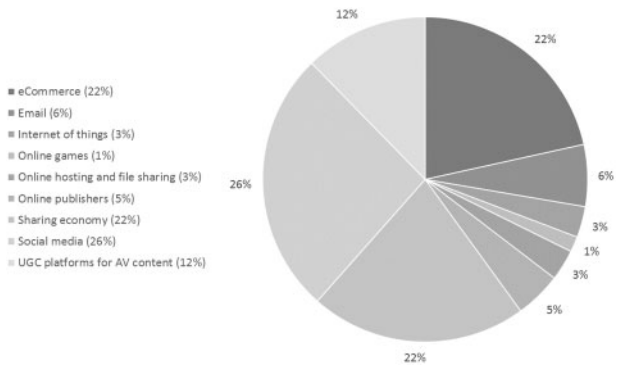

Figure 1. Overview of the investigated sectors.

48 As such, the research did not account for potential differences arising from the use of different interfaces (eg through a smartphone app; a mobile-friendly website; desktop website; etc.).

49 This initial phase of the research builds on a large body of already existing work, specifically aimed at analysing privacy policies. See, for example: Jamila Venturini and others, *Terms of Service and Human Rights: An Analysis of Online Platform Contracts* (Revan 2016) <http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/terms_of_services_06_12_2016.pdf> accessed 8 February 2018; Brendan Van Alsenoy and others, 'From Social Media Service to Advertising Network. A Critical Analysis of Facebook's Revised Policies and Terms', 25 February 2015 <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf> accessed 8 February 2018.

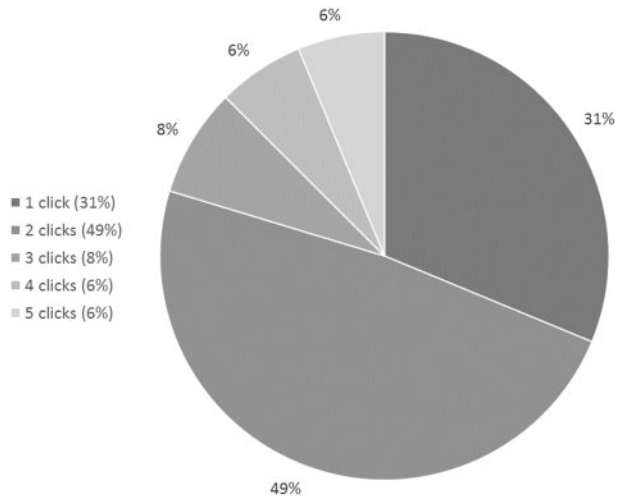

Figure 2. Number of clicks it takes to get from the homepage to the privacy policy.

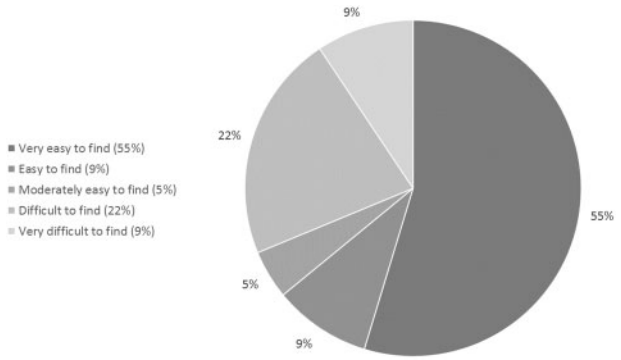

Figure 3. Ease with which the privacy policies were found.

Completeness. With regard to the quality and completeness of the information contained in these privacy statements, the study shows mixed results. Only just over half (53 per cent) were deemed (very) satisfying (Fig. 4). This may be explained by texts being excessively long or short: 20 per cent contained either less than a 1000 words or more than 5000 words (Fig. 5). Coupled with problematic structure and the use of legalese, nearly half of the investigated online service providers therefore failed to offer an approachable privacy policy. When compared to the requirements laid down in Articles 11–12 Directive 95/46 and Articles 13–14 of the GDPR, nearly all policies appeared to lack at least some mandatory information. For example, only 73 per cent of privacy policies clearly mentioned the name and contact details of the controller or its representative, 82 per cent pointed out the existence of the right of correction and 90 per cent provided a list of recipients or categories of recipients that receive personal information (Fig. 6). Several multi-faceted online service providers only offered one single privacy policy covering all of their services. Even if such consolidation might arguably bring users more clarity, it still raises concerns as to the completeness and specificity of the policy, and, consequently, as to the controller's compliance with the basic principles governing the processing of personal data.[50] Having said all that, just over half (53 per cent) of investigated privacy policies was still considered (very) satisfactory by participants (notably for carefully and intelligibly detailing the personal data collected, its source, purposes of processing, lawful grounds and/or the third parties to whom data are or may be disclosed).[51] The mismatch between this number and the earlier observation that nearly all policies were lacking at least some required information, does indicate an important issue: a reader-friendly privacy policy may nudge/mislead data subjects into a limited construction of (the scope of) their rights and/or extent of data processing.

Locating and reading privacy policies is essential when it comes to data subjects' informational empowerment. They should contain all the necessary details to identify and contact controllers, effectively enabling data subjects to exercise their right of access. With regard to online service providers in particular, such privacy policies generally constitute the primary way to obtain that information. Additionally, privacy policies also serve as the basis for evaluating the practical operation of the service as laid bare by access requests for example. In light of all this, there still seems to be some reason to worry about the continued—albeit moderate—issues regarding clarity, accessibility, and completeness of privacy policies.[52]

50 The most well-known example of issues related to the combining of privacy policies is provided by Google's legal struggles after it announced doing just that back in 2012. The French CNIL was appointed by WP29 to lead an investigation aimed at assessing Google's compliance with European data protection law. The final report underlined several legal issues with the new privacy policy such as a lack of information about the purposes and categories of data processed, renewed concerns about the combination of data across Google's different services and the absence of a clearly-determined retention period. For more information, see: Art 29 Data Protection Working Party, Report to Google following the CNIL investigation (16 October 2012) <https://dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf> accessed 8 February 2018; Judith Rauhofer, 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New PRIVACY Policy Raise Concern for the Future of the Purpose Limitation Principle?' (3 May 2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601463> accessed 8 February 2018; Rick Mitchell, 'Article 29 Working Party Urges Google To Reconsider Privacy Policies by Year's End', *Bloomberg BNA* (22 October 2012) <https://www.bna.com/article-29-working-n17179870400/> accessed 8 February 2018.

51 This number indicates the proportion of well-designed and/or user-friendly privacy policies, rather than fully compliant ones.

52 See references in n 49. The same conclusion regarding the existence of a duty to care on controllers was reached in the 10-country European study led by Clive Norris and Xavier L'Hoiry. See: Clive Norris and

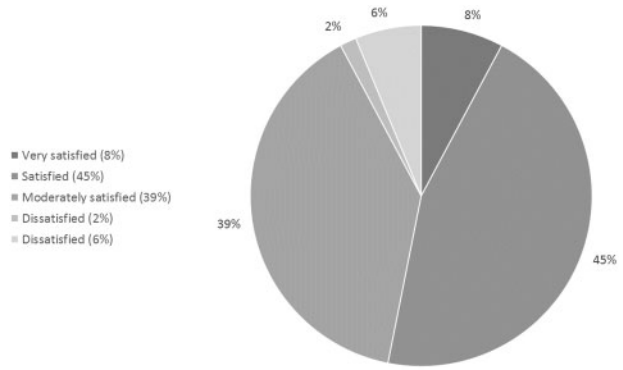

Figure 4. Satisfaction rate for privacy policies.

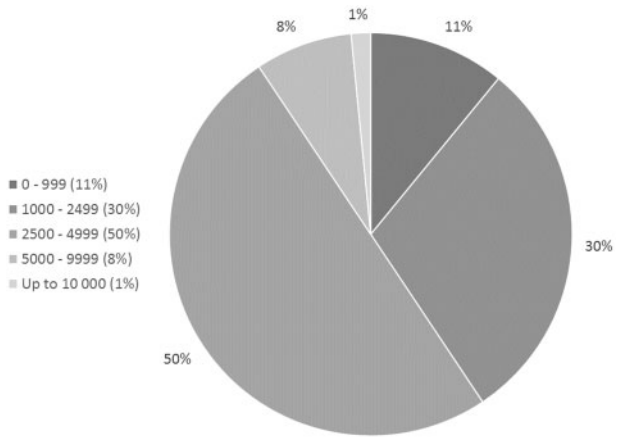

Figure 5. Word count for the privacy policies.

Filing access requests

Mention of the right of access in the privacy policy. Assuming that data subjects manage to locate and understand the service provider's privacy policy, they still need to know how to effectively exercise their right of access. Two main questions were assessed: (i) is the right of access specifically mentioned? and (ii) where/how should such a request be sent? Regarding the first question, it is worth recalling that Articles 10(c) and 11(1)c of Directive 95/46 (Articles 13(2)b and 14(2)c GDPR) oblige controllers to mention the existence of such a prerogative in their privacy policy. Worryingly though, 14 per cent of the investigated service providers failed to do so (Fig. 7). Some merely referred to the possibility of editing or deleting one's profile via the platform or 'contact them for further information on the privacy policy'. Others were completely silent on the matter. Only 66 per cent of the investigated providers provided clear instructions for exercising the right of access. While failing to specify the practical modalities for exercising the right of access may not violate Directive 95/46, this is likely to change with the GDPR which obliges controllers to '*facilitate the exercise of data subject rights under Articles 15 to 22*'.[53] It can therefore reasonably be assumed that providing a clear procedural scheme to data subjects willing to exercise their right of access will be part of controllers' new set of duties under the GDPR (below).

Means of communication. The answer to the second question partially echoes the above-mentioned numbers. For those cases where the right of access was specifically mentioned in the privacy policy together with clear instructions (66 per cent), sending access requests was a straightforward exercise. In the remaining cases, alternative means of communication had to be relied on, such as email addresses or contact-forms (either general-purpose or privacy-dedicated) (Fig. 8). Unsurprisingly, requests received faster support when privacy-dedicated contact points were approached. Fourteen per cent of service providers offered, among the list of means of contact, a postal address to send the access requests to, some even outside Belgium (where the data subjects were located). While the electronic form was always privileged whenever available, on four occasions (6 per cent) postal letters had to be sent as it was the only option to effectively exercise the right of access. Indeed, two controllers would only accept access requests if sent via postal letter. Furthermore, two eCommerce platforms only offered electronic support via contact forms to data subjects who had a pending or a past order on their website. Without a valid order number, it was therefore practically impossible to contact them other than through regular mail. Such a requirement may be considered quite restrictive, discouraging and disproportionate, especially in light of the service being exclusively offered online. Moreover, virtually all providers are collecting non-registered users' personal data as well (even if only through installing cookies or collecting IP addresses when visiting their website).[54] Nevertheless, many only allow an access

Xavier L'Hoiry, 'Exercising Citizens Rights Under Surveillance Regimes in Europe – Meta Analysis of a Ten Country Study' in Clive Norris and others (eds), *The Unaccountable State of Surveillance* (Springer International Publishing, Cham, Switzerland 2017) 415, point 14.1.5.

53 Art 12(2) GDPR. The exact meaning of what will constitute a facilitative practice is not clear today. This will be further specified by national DPAs, national courts and the European Data Protection Board once the GDPR enters into force.

54 On the legal issues emerging from the tracking of non-users in the social media context in particular, see: the technical report prepared for the Belgian Privacy Commission: Güneş Acar and others, 'Facebook Tracking Through Social Plug-Ins' (24 June 2015) <https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf> accessed 8 February 2018.

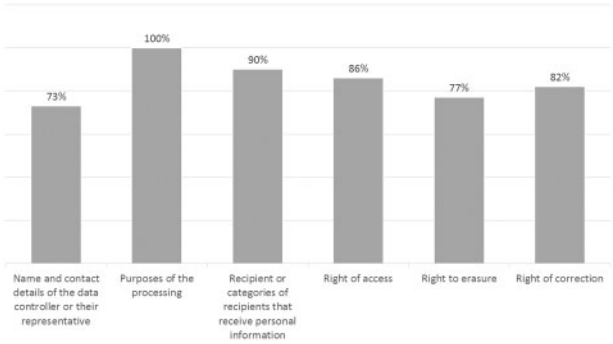

Figure 6. Information provided by controllers in their privacy policy.

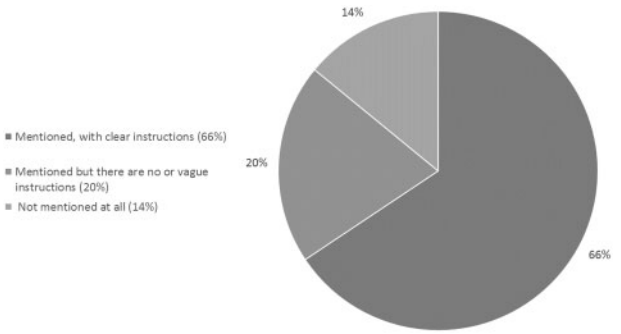

Figure 7. Specific mention of the right of access in the privacy policy.

request to be filed through a contact point made exclusively available to registered users. In such situations finding alternative means of reaching the controller can often be considered unreasonable and disproportionate, not to mention using such alternative means may often prove ineffective. Overall, the issues encountered in trying to contact controllers are tackled (at least in theory) in the GDPR, which suggests that controllers '*shall facilitate the exercise of data subjects' rights under Article 15 to 22*' (Article 12(2) GDPR) and '*should provide means for requests to be made electronically, especially where personal data are processed by electronic means*' (Recital 59 GDPR).

Corresponding with controllers

Necessity of correspondence. The access requests generated a wide variety of reactions, ranging from very good to very poor. Firstly—and as anticipated—none of the investigated controllers provided a one-shot complete answer (if an answer was received at all, see below).[55] In every case it was necessary to further engage with the relevant person or department (in charge of privacy and data protection issues), or with customer service, in order to obtain a satisfactory answer. As illustrated below, such interactions were sometimes particularly lengthy and frustrating. Whether as a deliberate avoidance strategy or due to simple ignorance, initial responses often only contained very basic information and/or requested to specify what data to send (even if the request referred to all information listed in Article 12(a) Directive 95/46). Somewhat ironically, one popular search engine even explicitly asked to help them locate the respective personal data. Most of the time, that first patchy answer did not explain why some information was missing. As such, data subjects effectively bear the burden of challenging the response's adequacy on the basis of little to no factual evidence of its incompleteness. In sum, these types of answers can be considered very problematic, as the rationale of the right of access is to uncover what personal data are being processed (and how) in the first place.

Proof of identity. Some service providers in the study asked for identity confirmation by sending them a copy of an official document such as an ID card or driving license before further processing access requests. While this might be considered a legitimate requirement (eg to prevent such abuse by an impersonating spouse), data subjects may also feel unconformable with having to disclose even more information in order to exercise their rights. This may especially hold true when—as was the case with regard to several investigated service providers—controllers do not accept redacted (eg covering some parts) or unofficial (eg student or loyalty cards) proofs of identity. Norris and L'Hoiry refer to this issue as the 'visibility paradox'.[56]

Delay and misunderstanding. Many providers completely ignored the first query so that (multiple) reminders were necessary before even having a request processed by controllers. When finally responding to the access request, several providers merely referred to their privacy policy or to the possibility of editing one's profile via their online platform. Finally, some providers did not understand the requests or questioned the existence and scope of the right of access. For instance, reactions such as the following were encountered:

> 'Good day. I don't really understand your request; do you want us to erase your data?'

55 In 87% of cases, it was even necessary to take extra steps before obtaining a mere reaction from the controller, independently of the necessity to engage in a correspondence to obtain a complete answer (eg send reminders, provide further details on the nature of the request, etc.).

56 Norris and L'Hoiry (n 52) 449–50, point 14.2.7: 'The Visibility Paradox'.

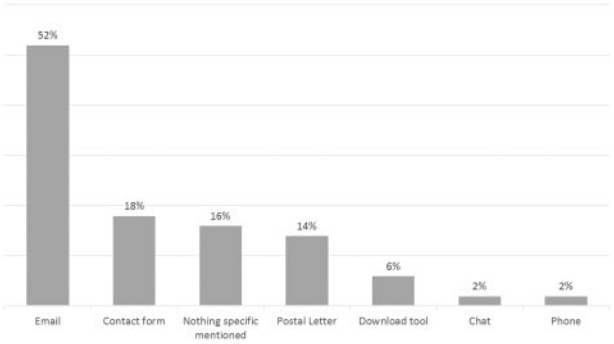

Figure 8. Specific ways mentioned in the privacy policy to exercise the right of access.

or:

> 'Hello. My name is ***** and I am a member of ***** Trust & Safety Team. For detailed information, you can, provide a court-ordered subpoena. You may submit the subpoena by going here: https://*****. That will forward your request to the appropriate department and they can respond to you directly'.

Obstacles—organizational burdens. The interaction with controllers (necessary in order to obtain satisfactory answers) proved to be even more arduous than expected. First, a series of organizational burdens was encountered that would easily discourage regular data subjects to proceed. Especially the need for back-and-forth correspondence with controllers made the whole process slow and time consuming. Trying to engage in a constructive and in-depth dialogue was also considerably complicated by the fact that some controllers redirected follow-up emails to different officers. It was therefore necessary to re-explain the context of one's request each time clarifications were sought on previous enquiries. Especially in cases where contact forms were used to get in touch with controllers, answers oftentimes lacked contact details forcing us to reopen new tickets for every subsequent claim. In other cases, these tickets were spontaneously closed by controllers having self-assessed that they had provided satisfactory answers. As mentioned earlier, reminders had to be sent frequently to controllers who ignored either initial requests or further correspondence. Our findings seem to confirm what was already suspected by Norris and L'Hoiry in their study, ie that such behaviour often constitutes an avoidance strategy rather than merely a result of poor administrative management.[57] Nonetheless, the study did also bring to the front some best practices such as fast responsiveness, helpfulness and the absence of any bureaucratic delay (see also below).

Obstacles—suspicion, irritation, and bad faith. In some instances, access requests were perceived and reacted to quite badly. While a majority of controllers remained neutral, some controllers showed suspicion, irritation, reluctance, and even bad faith in follow-up correspondence to access requests. In some instances, data subjects were given the feeling that their demands were not welcome or even illegitimate. Sometimes the attitude of the contact person was so unpleasant that regular data subjects would probably have given up the process. For instance, an important sharing economy platform provided these answers following an access request:

> 'Good morning. ***** being a masculine name, "Dear Sir" will suffice. We really don't have time for this; please look at our privacy policy, all your questions are answered. If you wish to erase your data, you are perfectly entitled to'.

When questioned about the progress of the access request, that same provider replied:

> 'I can't manage to motivate the developers' (translated from French).

When confronted with the same request, another sharing economy platform provided a rather disrespectful and aggressive answer despite the query being detailed and polite:

> 'To be honest, you are asking us to provide information we don't track. In other words, it would require us to start tracking information we don't collect or is not available on a personal level for the sole purpose of providing this information. All required information is made available in our privacy policy. If you think it's insufficient or believe ***** is not trustworthy, we're happy to delete your account and all related data. If you would like to use the site, then you automatically accept our user agreement and privacy policy. Last but not least, as far as we can tell, you haven't used the site (no booking, no messages, no profile). We receive this type of question once or twice a year, and it always comes from people who have no intention of being active on *****. So if you have a real concern, we're happy to explain more info'.

When explained to the platform that such a request, in addition to being legitimate in light of European data protection legislation, had been raised in the context of an empirical study aimed at analysing compliance with Directive 95/46, the following answer was given:

> 'Dear user, Thank you, but we haven't asked for that service. We have experienced legal councils both in our advisory board (people who work for *****) as well as law firms who keep us up to date about worldwide legislation'.

57 Norris and L'Hoiry, (n 52) 440.

and:

> 'This type of legislation is the reason we incorporated ***** in the US and not in Belgium. In reality, real users never ask for this type of information. They just delete their account. Our work is to [...] in the most trustworthy way. We have now deleted your account and have no data on file anymore, apart from this email in a separate customer support system. We have hereby fulfilled your request. And for all clarity: we treat real users and their privacy with the utmost respect. But we don't spend expensive resources to respond to frivolous requests'.

One controller in the empirical study simply admitted its non-compliance with data protection rules and replied:

> 'Thanks for reaching out. We do not yet offer full erasure of member data. We are reviewing the GDPR and will be fully compliant by May 25, 2018, the date of application'.

As demonstrated by the quoted answers, several controllers interpreted access requests as erasure requests. Some even proactively deleted an account even though only access was requested. Moreover, the above answer also illustrates ignorance as to the scope of current law. Indeed, when pointed to the fact that a right to erasure already existed under Directive 95/46 and in the relevant national transposing act, that controller merely answered:

> 'At this time, we don't have a system or process in place to manually delete member data from all of its stored location. It is something we are working on, however, You are welcome to update your and amend your data as needed, but I'll be unable to fully delete it at this time'.

Even though scarce, it should still be acknowledged that some controllers did demonstrate kindness and helpfulness throughout the whole access process, anticipating needs and providing proper support. Still, in general, interaction with controllers proved to be time-consuming, frustrating and eventually not fully satisfactory. In more than half (56 per cent) of cases, the overall process was deemed 'difficult' or 'very difficult' (Fig. 9).

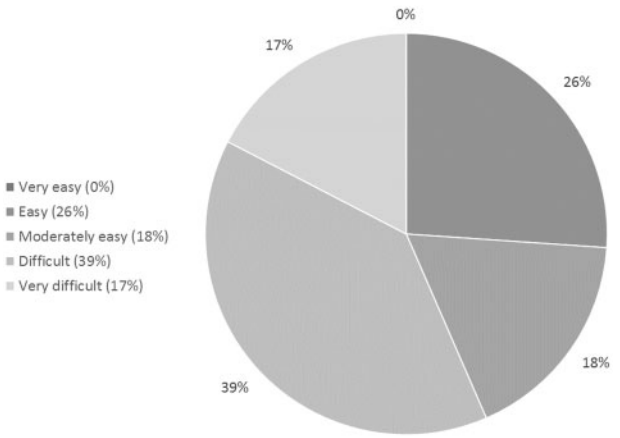

Figure 9. Ease with which the whole access process was conducted.

Quality of the answer

Number of replies and delay in replying. After five months, when it was decided to bring the empirical study to an end, only 74 per cent of the investigated online service providers had responded, whether with a satisfying answer or not. In other words, 26 per cent of them remained completely silent despite multiple reminders.[58] As a result, the amount of responses being assessed as part of the empirical study was already reduced by nearly a quarter compared to the number of providers contacted. The delay in responding to queries also appeared problematic in a significant number of cases. Thirty-six per cent of responses arrived more than 30 days after the initial request had been sent (Fig. 10). At the time of the empirical research, legal time limits depended on national implementing acts. This will, however, no longer be the case once the GDPR enters into force (below). It seems fair to say that such lengthy procedures and the general reluctance encountered with controllers considerably deter data subjects in persisting with their quest for access.

Completeness. Looking at the actual answers received, several issues emerged. As already alluded to above, in almost every case it was doubtful whether the response (especially the initial one) was complete. While this remains very hard to prove for a data subject, some indication may be given by comparing the answer with the respective privacy policy, monitoring the number of third-party trackers when visiting the service provider's website, and/or cross-checking descriptions of the provider's technical operations if available. Still, it remains difficult for data subjects to challenge the adequacy of responses to access requests without facing (pretended) incomprehension or ignorance from controllers. All in all, 67 per cent of responses received were considered insufficient (Figs 11 and 12).[59]

Form. Several issues can also be observed with regard to the format of controllers' responses. While a clear

58 The empirical study did not foresee specific instructions for sending reminders (ie at regular intervals). That being said, reminders were sent at the very least every month and generally more often than that.

59 To assess the completeness of the answers provided, all the personal data disclosed during the registration process was compared to what was disclosed by controllers following the access requests. The presence of third-party trackers (ie third-party to whom our data may have been transferred) was also monitored with the help of internet browsers add-ons such as Ghostery.

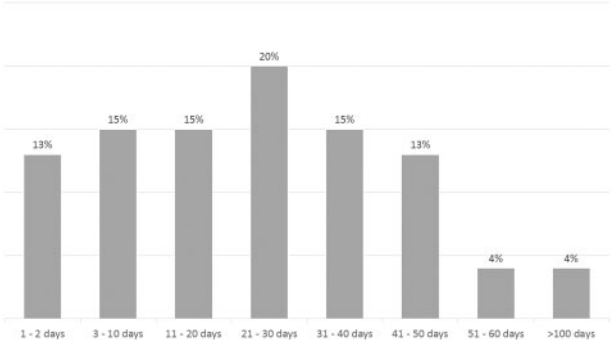

Figure 10. Days controllers took to respond.

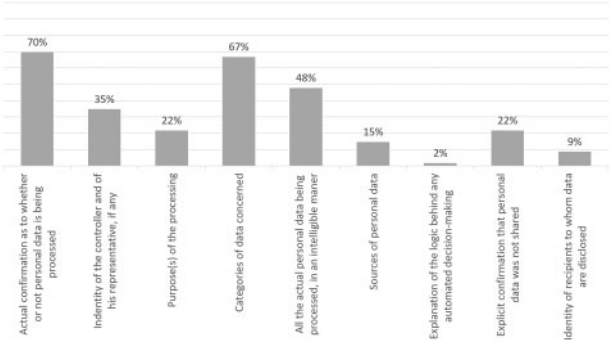

Figure 11. Information effectively provided following the access requests.

majority (80 per cent) relied on email exchanges (Fig. 13), there were some differences as to the way content was displayed. Some of them included the respective personal data as actual text in the body of their emails which was easier to browse but lacked structure and clarity. Others attached a PDF or Excel document which allowed for more comprehensiveness, but may be problematic from the point of readability (PDFs for machines and Excel documents for humans). Some attachments only contained raw data seemingly extracted straight from the controllers' databases, and others were organized in a more user-friendly manner. Twelve per cent of the investigated providers made the relevant documents available through a URL which, for some, expired after a certain period of time and therefore offered less durability than traditional email attachments (though could be seen as a security measure as well). Finally, answers provided through a dedicated 'download my data' tool (only 4 per cent) proved to lack completeness in many ways.

Overview

Overall finding. Some best practices and positive experiences set aside, the empirical study suggests that the right of access as *theoretically* incorporated in EU data protection law does not generally fulfil its underlying rationale when *practically* exercised by data subjects. Answers provided were indeed rated (very) satisfactory in only 22 per cent of instances (Fig. 14). Such a disappointing—yet somehow unsurprising—outcome can be attributed to a series of reasons ranging from problematic yet easily remedied misconduct to situations of systematic non-compliance. Given the black-box nature of many controllers, it can be very hard to impossible for data subjects to establish that their rights (of access) have not been *fully* accommodated. Correspondence with controllers throughout the empirical study (eg questioning the reasons behind incomplete answers, etc.) did give an indication as to the reasons behind the many problems related to effectively exercising/accommodating access rights, the most important of which can be summarized as a lack of awareness; organization; motivation; and harmonization.

Lack of awareness. First and foremost, the empirical findings laid bare a worrying lack of awareness among controllers as to the existence and scope of data subject rights.[60] A good portion of controllers completely ignored or at least showed general discomfort when confronted with access requests. Even though the findings did not go as far as establishing unawareness of data protection law, they certainly demonstrated substantial misconceptions as to its full breadth. This was particularly well-illustrated by how most controllers seemed to interpret the notion of 'personal data' incredibly restrictively.[61] Indeed, as mentioned above, responses to access requests (especially the initial ones) generally only contained very little information, even in situations where controllers showed a willingness to cooperate. Moreover, many of the investigated controllers were not familiar with the modalities governing access requests. All in all, this lack of knowledge has rendered the exercise of the right of access lengthy, unpleasant and frustrating with very little satisfactory answers.

Lack of organization. Secondly, substantial deficiencies regarding the internal organization of controllers in light of data subject rights could also be observed. Most of the small- and medium-sized online service providers contacted did not have any department, team, or even

60 This element has also been underlined in Galetta, Fonio and Ceresa (n 41) 21 for Italy and 23 for Belgium.

61 Admittedly, the notion of personal data is a complex one. See most recently: Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law' (30 September 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355> accessed 8 February 2018

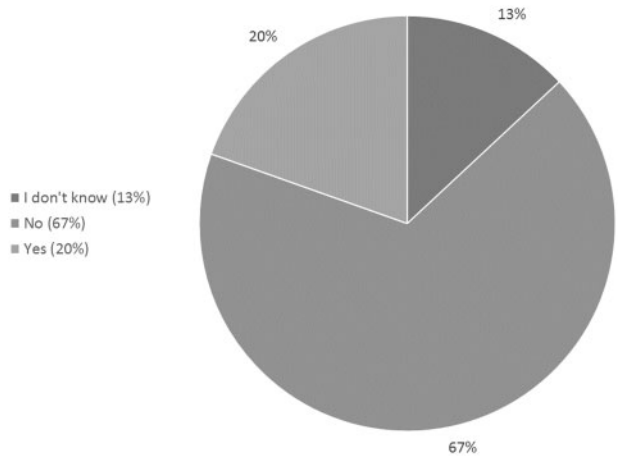

Figure 12. Does the response include all personal data you think the controller is processing about you?

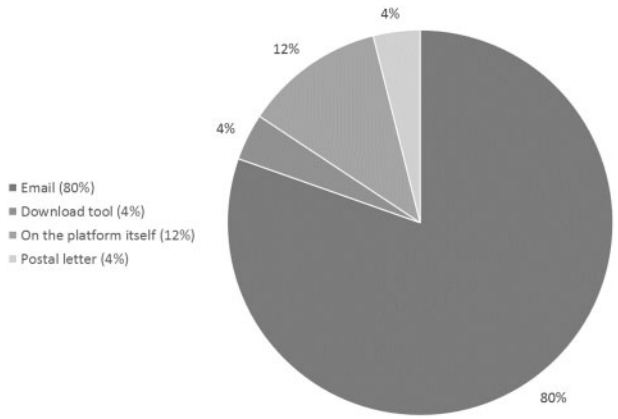

Figure 13. Medium used to provide answers.

person in charge of managing privacy—and data protection-related issues. Instead, a significant portion of requests was handled by customer service or redirected to the wrong officer. From a more technical perspective, some controllers struggled to identify and locate the personal data requested, simply because their storage methods fell short of offering clear and reliable ways to accommodate data subject rights. Several providers implicitly or explicitly argued that extracting the relevant pieces of information from their databases was difficult to impossible. This issue will only grow in importance as information processing eco-systems become increasingly intertwined and complex (eg in light of IoT developments). It is yet to be seen if the 'Data Protection by Design and by Default' provision in the GDPR (Article 25) can preserve adequate protection in the face of this trend. Indeed, a perverse reading of that provision could lead to justifying the design of one's systems to make it hard or impossible to retrieve personal data of a specific data subject. Providers of smart home assistants,[62] for example, may invest in encrypting, pseudonymizing and/or decoupling recordings, transcripts and metadata from the respective data subjects. Retrieving such data on an individualized basis may be difficult, but can this be used as a justification for not accommodating data subject rights? Such a reading of the data protection by design principle would seem to go against the very rationale of the GDPR.[63]

Lack of motivation. Thirdly, the empirical study suggests a considerable lack of motivation amongst a significant portion of controllers. General indicators of this were, for example, the number of days it took controllers to respond (with 71 per cent not providing any response within 10 days) and the necessity to take extra steps before even obtaining a simple reaction in 87 per cent of cases. Additionally, the amount of suspicion, bad faith, irritation, and disrespect encountered throughout, further suggest a general unwillingness to accommodate data subject rights. It is unclear (and hard to establish) to what extent this apparent lack of motivation is symptomatic of deeper, systematic issues regarding non-compliance with data protection rules more broadly.[64]

Lack of harmonization. Fourthly, the fragmented European legal landscape regarding data protection[65] did further complicate the filing, monitoring, and follow-up of access requests. In each case, it was necessary to delve into the relevant transposing national acts and into their interpretation by national courts and DPAs, to assess controllers' compliance with data protection law. The defining of legal time limits and introducing exemptions to the right of access remain entirely up to Member States and, therefore, are likely to vary depending on the law applicable to the provider. In other words, requesting access was a particularly demanding operation which required legal literacy, patience, and dedication.

62 *E.g.* Amazon Alexa, Google Now, Apple Siri, etc.

63 See also: Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (Article 29 Working Party 2017) Guidelines WP 251.

64 At least with regard to one investigated controller (an important supermarket chain in Belgium, the empirical study brought about a demonstrable change. More specifically, the company's privacy policy was updated shortly after correspondence with them in the context of this study (eg an explicit reference to the right of access was included).

65 See *inter alia*: Douwe Korff and Ian Brown, 'Comparative Study on Different Approaches to New Privacy Challenges , in Particular in the Light of Technological Developments' (European Commission—DG Justice 2010) Final Report.

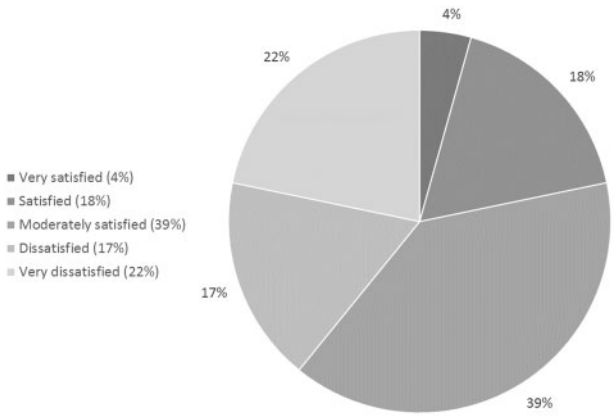

Figure 14. Satisfaction rate for the answers provided.

Concluding remarks. In sum, the empirical findings suggest that the lack of awareness, organization, motivation and harmonization, are among the main hurdles obstructing an effective exercise of the right of access and therefore thwarting the right's potent potential. Either data subjects are effectively denied access to their data (26 per cent of the access requests filed during the empirical study were not answered at all), or they face considerable obstacles trying to obtain a satisfying answer from controllers. This, in turn, often prevents (or at the very least curtails) data subjects' ability to exercise other key rights (eg correct, object, erasure).

The future. A new era for data subject rights?

GDPR. Paradigm Shift?

Information to be provided. The entry into force of the GDPR will drastically modify data protection across the EU, but how far will the right of access be impacted? Firstly, and as demonstrated in Table 1, more information will have to be provided by controllers (eg where possible, the envisaged retention period or the criteria used to determine that period, the existence of the right to rectification, to erasure, to restriction of processing and to object and the right to lodge a complaint with a supervisory authority). Adding mandatory categories of information that must be communicated to data subjects, only marginally increase the administrative and organizational burden on service providers who are already adequately dealing with access requests under Directive 95/46. Data subjects will presumably benefit from this expanded set of information, which, in turn, should boost their informational empowerment.

Practical modalities—under Directive 95/46. Secondly, and as pointed out in Table 2, the shift from Directive 95/46 to the GDPR has brought significant changes to the modalities governing the handling of access requests. The move to a Regulation mirrors the EU institutions' wish to build a '*strong and more coherent data protection framework [. . .] given the importance of creating the trust that will allow the digital economy to develop across the internal market*'.[66] Considering the relative absence of any practical requirements within Directive 95/46, every Member State had developed its own set of modalities framing the exercise of data subjects' rights (above). On top of legislative measures, national DPAs and domestic case law have further shaped the way data subjects and controllers should behave when confronted with such requests. In other words, Directive 95/46 has not driven the development of uniform measures regarding the exercise of the right of access and there is currently no European-wide comprehensive and authoritative guidance on governing its practical application (neither from the WP29 or the CJEU).

Practical modalities—under the GDPR. The GDPR echoes the above-mentioned issue right from the start. Reminding us that Directive 95/46 '*has not prevented fragmentation in the implementation of data protection across the Union*', it then underlines that an '*effective protection of personal data requires the strengthening and the setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data*'.[67] In other words, the European legislator clearly intended to parry the lack of practical harmonization resulting from 28 separate legal frameworks by providing concrete, well-defined modalities for exercising data subjects' rights.[68] Among them, Article 12(5) *j* Recital 59, empowers data subjects to request access free of charge and constitutes an important improvement to the current status quo.[69] The same

66 Rec 7 of the GDPR.

67 Recitals 9 and 11 of the Directive 95/46, respectively.

68 Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2017) Computer Law & Security Review 4.

69 Under Directive 95/46, controllers can charge a fee provided that it is not 'excessive' (art 12a), ie fixed at a level that is likely to constitute an obstacle to the exercise of the right of access' (*X*, Case C-486/12 (ECLI:EU:C:2013:836), para 29). For example, the maximum amount that can currently be charged by controllers in the UK is 10 pounds (see: ICO Guide to Data Protection, 48, <https://ico.org.uk/for-organisations/guide-to-data-protection/> accessed 8 February 2018). Considering the amount of online platforms involved in the processing of personal data, such a fee can easily act as a deterrent for data subjects willing to obtain access from different actors.However, the GDPR allows controllers to charge a reasonable fee in two situations. First, when requests are

Table 1. Information to be provided under the right of Access

		Directive 95/46	GDPR
		Rec 41–44; Art12(a)	Rec 63,64,73; Art 15
Confirmation as to whether or not personal data are being processed		✓	✓
The purposes of the processing		✓	✓
The categories of personal data concerned		✓	✓
Any available information as to the source of the personal data		✓	✓
The recipients or categories of recipient to whom data:	Are disclosed	✓	✓
	Will be disclosed		✓
Regarding automated decision-making producing legal effects or significantly affects the data subject	Its existence	(implied)	✓
	Its logic	✓	✓
	Its significance		✓
	Its envisaged consequences		✓
Where possible, the envisaged retention period or the criteria used to determine that period			✓
The existence of the right to rectification, to erasure, to restriction, and to object			✓
The right to lodge a complaint with a supervisory authority			✓
Where personal data are transferred to a third country or an international organization, the appropriate safeguards relating to the transfer			✓

can be said for the newly introduced one month time limit within which controllers must answer access requests (Article 12(3)-(4) *j* Recital 59). Finally, by suggesting matching the way personal data are processed with the way access should be offered, Recital 59 also aims to prevent controllers from discouraging data subjects in their attempts to obtain access by using other means, such as postal letters, to answer their request. Clearer, well-defined and harmonized practical modalities will greatly contribute to facilitate the exercise of the right of access. Indeed, fragmentation raised considerable uncertainties during the empirical study, requiring investigating national specificities when assessing controllers' compliance with domestic transposing acts. Although the GDPR does not harmonize the way national DPAs will handle the complaint process itself (Article 61 merely implements a general duty of mutual assistance to foster the consistent application of the framework), commonly shared practical modalities will prove very valuable in the context of trans-border right of access dossiers.

Limitations. The GDPR is no silver bullet though. Firstly, some of the terms used in the new text remain open to interpretation. This is especially true with regard to Article 15(4) and Recital 63 which specify that '*the right to obtain a copy [of one's personal data] shall not adversely affect the rights and freedoms of others*'. Secondly, Article 23 leaves it up to Member States to define restrictions to data subject rights, potentially re-introducing fragmentation through the backdoor.[70] As a result, data subjects' access requests might

manifestly unfounded or excessive, in particular because of their repetitive character (art 12(5)a). What must be considered 'excessive' or 'repetitive' is somewhat unclear and remains to be seen. Second, for any further copies of the personal data requested by the data subject (art 15(3)). Again, it is unclear whether this provision applies to any subsequent copy, whether *digital* or *physical*, or only to further *physical* copies. When considered together, these two exceptions could also overlap in the case of subsequent requests. If a controller indeed fails to charge a reasonable fee on the basis of the request being repetitive, he could also try to levy such a fee by alleging that the subsequent request amount to a further copy of previously requested data (and *vice versa*). However, providing an *ex ante* answer to these questions remains complicated.

70 The '*one single law applicable across the EU*' promise is therefore not entirely true as it was underlined in the European Commission Factsheet, 'How will the EU's data protection reform strengthen the internal market?' <https://ec.europa.eu> accessed 8 February 2018. It must be said that the legislator did install some safeguards. Ie Art 23(1) specifies that restrictions should '*respect the essence of the fundamental rights and freedoms*' and be '*necessary and proportionate in a democratic society*'. See also Table 2.

Table 2. Specified modalities for exercising the Right of Access

	Directive 95/46	GDPR
Fee	Art 12(a): **without** [. . .] **excessive** [. . .] **expense**.	Rec 59; Art 12(5)1: obtaining access must be **free of charge**, with **two exceptions**: • Art 12(5)1(a): possibility for controllers to charge a reasonable fee where requests are manifestly unfounded or excessive; • Art 15(3): possibility for controllers to charge a reasonable fee for any further copies requested.
Time limit	Art 12(a): **without** [. . .] **excessive delay**.	Rec 59; Art12(3)-(4): whether the controller intends to take action or not, answer to the data subject **without undue delay** and, in any event **within one month of receipt of the request**. Possibility to extend that period by **two further months** where necessary, taking into account the complexity and the number of the requests.
Form (request)	Not addressed by the Directive	Rec 59: controllers should provide means for requests to be made **electronically**, especially where personal data are processed by electronic means.
Form (answer)	Not addressed by the Directive	Rec 63; Art 12(1): the information shall be provided **in writing**, or **by other means**, including, where appropriate, **by electronic means**. Where possible, **direct remote access** to a secure system should be made available. When requested by the data subject, the information may be provided **orally**, provided that the identity of the data subject is proven by other means.
Intelligibility	Art.12(a)2nd indent: in an **intelligible form.**	Rec 58; Art 12(1): in a **concise**, **transparent**, **intelligible** and **easily accessible** form, using **clear and plain language**, in particular for information addressed specifically to a **child**.
Verification of identity	Not addressed by the Directive	Rec 64; Art 12(6): the controller **may** request provision of additional information necessary to confirm the identity of the data subject, and **should** use all reasonable measures to do so, in particular in the context of online services and online identifiers.
Limitations	Rec 43; Art 13(1): Member States may adopt **legislative measures** to restrict the scope of the obligations and rights provided for in **Arts 6(1), 10, 11(1), 12 and 21** when such a restriction constitutes a **necessary measure** to safeguard: see list Art 13(1)a-g.	Rec 73; Art 23(1)-(2): Union or Member State law may restrict by way of a **legislative measure** the scope of the **obligations and rights provided for in Articles 12 to 22** when such a restriction **respects the essence of the fundamental rights and freedoms** and is a **necessary and proportionate measure in a democratic society** to safeguard: see list Art 23(1)a-j. These measures must contain **specific provisions** at least, where relevant, as to: see list of Art 23(2)a-h.
	Art 13(2): subject to **adequate legal safeguards**, Member States may, where there is **clearly no risk of breaching the privacy of the data**	Recital 153; Art 85(2): for processing carried out for **journalistic purposes or the purpose of academic artistic or literary expression**, Member States shall provide for exemptions or derogations from Chapter

Continued

Table 2. Continued

	Directive 95/46	GDPR
	subject, restrict by a **legislative measure** the rights provided for in Article 12 when data are processed **solely for purposes of scientific research** or are **kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics**'.	III (rights of the data subject) if they are **necessary to reconcile the right to the protection of personal data with the freedom of expression and information**. Rec 156; Art 89(2): where personal data are processed for **scientific or historical research purposes or statistical purposes**, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the **conditions and safeguards referred to in Art 89(1)** in so far as such rights are **likely to render impossible or seriously impair the achievement of the specific purposes**, and such derogations are **necessary for the fulfilment of those purposes**.

effectively be treated differently depending on the country where the controllers are located, further complicating the practical exercise of data subjects' rights in general.[71]

Concluding remarks. In sum, the GDPR is a game changer in many ways. First of all, it will bring more clarity regarding the practical operation of the right of access, even if it does not guarantee full harmonization per se. Generally, therefore, data subjects will not have to deal with a messy patchwork of domestic transposing acts anymore, with some providing clear modalities and others remaining completely silent. Establishing strict and straightforward procedural requirements shared across Member States is thus a welcome addition that will certainly boost legal certainty. Secondly, the way the GDPR is going to be interpreted by national DPAs and domestic courts is likely to show more consistency throughout Member States.[72] With this in mind, the GDPR at least has the potential to significantly fortify informational empowerment of data subjects.

Is there still a role for data subject empowerment?

Some scepticism. Data subject empowerment, or individual control over personal data, is often decried as being ineffective and obsolete.[73] This claim seems to be confirmed by the empirical evidence described above. Even when overcoming all of the practical hurdles and the data subject receives an answer to his/her access request, it will often be incomplete, hard-to-understand and not very useful (eg to truly understand *what* is done with one's data and *why*). Given the observation of current practices, one may remain sceptical as to how much the GDPR will tackle these concerns in the field.[74]

71 The GDPR foresees many other flexibilities, with varying impact on the right of access. For an overview, see for example: Amberhawk Training, 'How "Flexible" Can the UK Actually Be on EU Data Protection Law?'(4 May 2016) <https://www.theregister.co.uk/2016/05/04/will_the_uks_approach_to_the_gdpr_be_harmonised/> accessed 8 February 2018; Diego Naranjo, 'Proceed with caution. Flexibilities in the General Data Protection Regulation' (5 July 2016) <https://edri.org/analysis-flexibilities-gdpr/> accessed 8 February 2018; Detlev Gabel, Tim Hickman, 'Chapter 17: Issues subject to national law – Unlocking the EU General Data Protection Regulation' in *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law* (White&Case) <https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection> accessed 8 February 2018. See also Winfried Veil's map on the opening clauses in the GDPR <https://www.flickr.com/photos/winfried-veil/24134840885/in/dateposted> accessed 8 February 2018.

72 Art 63 GDPR. Also see below.

73 See *inter alia*: Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250; Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 SCRIPTed <http://script-ed.org/?p=1927> accessed 8 February 2018.

74 For a constructive counter-argument, see: Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the Obstacles to Privacy Self-Management Be

Combined with the general 'control fatigue' of most individuals today, it is indeed fair to question the added value of many individual empowerment rights indeed.

Dusting off the right of access. We are of the strong opinion that there is still an important role to play for data subject rights, enabling individual control over personal data. The right of access in particular, can be seen as a key provision in this regard. It generally constitutes the first logical step in exercising any other data subject right (above). Indeed, before invoking the right to object, erasure, correction, or portability for example, one will first need to know what data is processed exactly and what for.[75] Secondly, the right of access may well become an important tool to monitor and enforce data protection compliance, in light of under-resourced data protection authorities. The accountability principle and risk-based approach in the GDPR risk to become empty shells without effective enforcement. In light of all this, data protection compliance by controllers, hinges on data subject empowerment.

Vindicating data subject rights. Data protection law aims to achieve the control rationale (as laid down in Article 8 Charter),[76] *inter alia* through a variety of data subject empowerment measures. These measures operate both at an *ex ante* and an *ex post* stage. *Ex ante* empowerment measures aim to give data subjects control *before* processing initiates (eg consent in Article 6(1)a and Article 7 GDPR), while *ex post* empowerment measures do so *after* processing has initiated (eg rights to erasure and to object in Articles 17 and 21 GDPR).[77] What makes the latter so valuable in increasingly complex data processing eco-systems is that they are designed with time in mind. They inherently enable control throughout personal data's lifecycle. Data protection does not stop at the moment it is collected.[78] Enabling individuals to control (the use of) their personal data over time is important for a variety of reasons. Today, it is practically impossible to predict (all) (negative) consequences of the use of personal data.[79] Even if one can foresee a few, they are very abstract, distant and uncertain.[80] *Ex ante* data protection empowerment measures (consent in particular)[81] are not sufficient to enable an adequate—persistent through time—level of control over data.[82] This is particularly true given the increasing ambiguity regarding the data protection framework's material scope.[83] *Ex post* measures offer people an effective opportunity to permanently (re-)evaluate the use of their data for ever-changing purposes in dynamic contexts.[84] The right of access—as well as other data subject rights—give teeth to general principles of fairness, accountability, and responsibility.[85]

Collective control. The control narrative in data protection law should not be read rigidly as only including *individual* control, entirely dependent on a data subject's active engagement.[86] Put differently, data subject rights should not be depicted as serving only a handful of exceptionally motivated people. Control over personal data can be particularly powerful when exercised collectively. Collective legal action[87] and several grassroots initiatives[88] aim to facilitate the effective exercise of data subject rights by joining forces and making the whole process much more scalable. Deploying data protection rights *en masse*, could also resolve broader

Overcome? Exploring the Consent Intermediary Approach' (2017) 4/2 Big Data & Society 1.

75 See in this regard also: Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (art 29 Working Party 2013) 03/2013 14 <https://ec.europa.eu> accessed 8 February 2018.

76 Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law (*forthcoming*).

77 See also: Jef Ausloos, 'The Interaction between the Rights to Object and to Erasure in the GDPR' <https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/> accessed 8 February 2018.

78 See for example: Art 29 Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (art 29 Working Party 2014) Opinion WP 223 3 <https://ec.europa.eu> accessed 8 February 2018.

79 Reconfirmed in: European Commission, 'Impact Assessment Accompanying the Proposals for General Data Protection Regulation and Directive on Data Protection in Police and Judicial Matters' (European Commission 2012) Commission Staff working Paper SEC(2012) 72 final.

80 Jef Ausloos, 'The "Right to Be Forgotten" – Worth Remembering?' (2012) 28 Computer Law & Security Review 143, 144–45.

81 Koops speaks of the 'mythology of consent'. See: Koops (n 73) 251.

82 'Because of the nature of information processing in today's hyper-connected network society, this layer of ex ante protection is becoming weaker and weaker.' In: Bart W Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 Computer Law & Security Review 45, 49. 'Privacy policies are written in vague legalese and people do not read them anyway. Network externalities, lock-in and the lack of valid alternatives often force people into consenting.' Ausloos (n 81 145.

83 The notion of 'personal data' has become very ambiguous and should not be seen as a static concept. Information can be (un)linked to a person over time, vis-à-vis different actors and in different contexts. A flexible and casuistic approach is required, taking into account the constant transformation of 'data' as such.

84 Not in the least in the context of the 'Internet of Things' where *ex ante* measures might be quite hard due to the lack of screens to interact with. In: Meg Leta Jones, 'Privacy without Screens & the Internet of Other People's Things' (2014) 51 Idaho Law Review 639, 653.

85 Clifford and Ausloos (n 76).

86 Ibid.

87 Now explicitly mentioned in the GDPR (art 80), though still subject to many unresolved questions. See *inter alia*: Maja Brkan, 'Data Protection and European Private International Law: Observing a Bull in a China Shop' (2015) 5 International Data Privacy Law 257, 263, 273.

88 See note 41.

societal 'collective privacy' challenges, stemming from power asymmetries (eg to equality or freedom of expression).[89] In light of this broader perspective, any institution or organization aimed at protecting rights or interests that are affected by personal data processing[90] may find ways to use data protection rights (particularly when exercised collectively) to further their case. In sum, the right of access may serve a wider, strategic role in raising awareness and advancing policy changes. Perhaps the most important example of this can be found in Max Schrems' (still ongoing) actions against Facebook, effectively resulting in the invalidation of the Safe Harbour agreement.[91]

Lessons learned

As underlined above (the sub-Section 'Is there still a role for data subject empowerment?'), the empirical study has highlighted a significant amount of issues with regard to exercising the right of access against information society service providers. Based on this, the present section aims to provide recommendations for controllers.

Visibility, readability, and content of privacy policies. Given the amount of research on this already,[92] it may seem like kicking in an open door, but it is still worth reiterating that many privacy policies still need to be improved considerably. Particularly in light of exercising data subject rights. Indeed, the empirical findings (re-)confirmed that the visibility and readability of privacy policies generally constitute the first stumbling blocks on the long and windy road to access. This is all the more troublesome since these policies are often data subjects' only source of information on how to exercise their rights. A step in the right direction would be to dedicate an entire section to data protection issues rather than spreading that information among other legal notices such as terms of service and/or cookie policies. That section should also be unequivocally titled and clearly visible on the provider's homepage to spare users the need to browse the entire website before stumbling upon the relevant information.[93] Controllers' internal organization should also not negatively impact data subjects' informational empowerment. The fact that a controller is part of a bigger group or relies on different platforms for all or part of its activities should not justify merely referencing another privacy policy that may often be too generic and unclear about how to exercise data subject rights. In the same vein, consolidated privacy policies dealing with different services should be avoided[94] and their accessibility on mobile apps should be as straightforward as for their desktop equivalent. Finally, controllers should articulate their privacy policy so that data subjects' rights are sufficiently visible. In the same vein, comprehensive information should be given as to their modalities of exercise and the outcome to be expected.

Handling of access requests—templates. On top of problematic privacy policies, the empirical study also brought to light shortcomings in the way access requests are handled. Even though numerous suggestions can be made for addressing these concerns,[95] two spring to mind as particularly relevant: a formal and a technical one. Firstly, controllers should provide straightforward templates to data subjects wishing to request access to their personal data. Throughout the empirical study, considerable uncertainties related to the form and content of requests, which in turn led to lengthy and often unfruitful correspondence with controllers. Allowing users to build their requests following a clear and predetermined format would dismiss many procedural concerns and reduce the element of surprise for controllers confronted with requests from multiple sources. Right from the start of the process, data subjects would therefore know exactly what documents to provide,

89 Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing, Cham, Switzerland 2017).

90 Eg from financial regulators and consumer protection agencies to environmental protection and anti-discrimination organisations. Trade unions (or organizations with similar goals) may be especially interested in gaining more fine-grained access to the data collected on drivers by platforms such as Uber or Deliveroo.

91 *Maximillian Schrems v Data Protection Commissioner*. See nn 37, 38 and 39.

92 See the references in note 48. See also for example the 2015 and 2017 corporate accountability indexes drafted by the non-profit research initiative 'Ranking Digital Rights' (RDR), <https://rankingdigitalrights.org/> accessed 8 February 2018. See also FH Cate, 'The Limits of Notice and Choice' (2010) 8 IEEE Security and Privacy 59–62; Lee A Bygrave, *Internet Governance by Contract* (OUP, Oxford 2015); Yannis Bakos, Florencia Margotta-Wurgler and David R Trossen, 'Does Anyone Read the Fine Prints? Consumer Attention to Standard-Form Contracts' (2014) 43 The Journal of Legal Studies; Nancy S Kim, 'The Duty to Draft Reasonably and Online Contracts', in Larry DiMatteo and others (eds), *Commercial Contract Law: A Transatlantic Perspective* (CUP, Cambridge, UK 2012).

93 In that sense, today's custom consists of placing a hyperlink redirecting to the privacy section at the bottom of the homepage together with the general details on the platform. While such a practice may be perceived as a way to conceal that text, it nonetheless constitutes a form of standardization which is likely to benefit data subjects.

94 See n 54 on the issues inherent to Google consolidating the privacy policies of its different services.

95 For a comprehensive overview of the impact the GDPR will have on the way controllers conceive and design their processing activities and a list of practical recommendations to adapt to these changes, see: Tikkinen-Piri, Rohunen and Markkula (n 68) 13–18, especially the table on p 14.

which information to attach and where to send their request. In other words, implementing such measures would benefit both parties, accelerate the access process, set reasonable expectations as to its outcome and illustrate online service providers' privacy-conscious intentions. Adopting such templates also makes it easier for DPAs to assess compliance with data protection law, in turn providing more legal certainty to the respective controller. Templates that (deliberately) misinterpret or reduce in scope the actual breadth of the right of access should be shunned as they misguide data subjects as to what they are legally entitled to receive.

Handling of access requests—technical overhaul. Secondly, controllers should adapt the technical functioning of their processing activities to better comply with the requirements governing access. Recital 63, for example, requires controllers 'to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data' whenever possible. Data protection by design and by default (Article 25) should be implemented so as to foster/facilitate accommodating data subject rights, and not interpreted in order to prevent their effective exercise (above). Providing data subjects with a fast, complete, and electronic answer to their request will often require a complete overhaul of the way personal data are collected and stored at the backend. The empirical study has indeed demonstrated that a significant number of controllers struggled to even identify and locate the requested pieces of information. This could be avoided by developing/reconfiguring their systems in such a way to facilitate the retrieval of relevant data in a secure and individualized way. Indeed, their systems should be designed in a way that enables the exercise of data subject rights. Ideally, this would go as far as to actively facilitate exercising such rights, for example through automating the process and ensuring information is machine-readable and interoperable (cf Article 20 on the right to data portability).[96] More than just a burdensome legal obligation or optional convenience, such a proper restructuring could also prove essential for large undertakings dealing with considerable amounts of requests, especially in light of the one-month time limit introduced by the GDPR. In sum, improving access therefore implies rethinking the processing itself.

Abuse. As with any other right, the right of access can be abused. A classic example perhaps being an impersonating spouse requesting access for dishonest reasons. Indeed, already in 1969 authors pointed to the risk of releasing other people's personal data and violating others' privacy by unthoughtfully accommodating access requests.[97] Some obstacles identified during the empirical research (eg requesting a scan of an ID card for identity verification) can therefore be deemed legitimate to prevent abuse and/or affecting others' rights or interests. Indeed, as mentioned before Article 15(4) and Recital 63 specify that the right of access should not adversely affect the rights or freedoms of others. Still, interaction with controllers in the empirical study suggest that in many cases hurdles were not (solely) aimed at preventing abuse, but rather served as strategic tools for avoiding access rights altogether. Examples of this include long response-times in combination with incomplete answers and the need for further interactions; arguments as to the scope of data protection law and in particular the definition of personal data; data protection by design measures; trade secrecy; and so on. In sum, while abusive access requests should certainly be prevented, this should not be used to justify not having to accommodate the right of access (and/or other data subject rights) altogether. Regular 'check-ups' such as in this empirical study enable mapping controllers' response strategies, call out bad actors and take action where needed (and possible).

Bigger picture

Improving the practical operation of the right of access does not solely hinge upon the revamped Article 15 GDPR (cf. above and Tables 1 and 2). It is also important to position the right within the GDPR as a whole,[98] as well as contextualize it against the broader socio-economic backdrop in which it operates.

Right to explanation. Among the elements introduced by the GDPR, one was particularly awaited and has raised quite some commentary in legal literature already: the so-called 'right to explanation' of decisions taken by algorithmic and artificially intelligent systems.[99] Scattered over several provisions of the Regulation—namely Articles 13(2)f and 14(2)g, 22(3)

96 'Download my data' tools are generally no panacea either. Apart from orienting users towards a pre-determined conception of what access should mean, their failure to include certain types of information has been criticised as well. This is notably the case for Facebook's download my data functionality which, according to *Europe v Facebook*, allows data subjects to retrieve '*only a fraction of all data Facebook stores about you*'. See: *Europe v Facebook*, 'Get your data!' <http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html> accessed 8 February 2018.

97 Miller (n 4) 1100.

98 And how it interacts with other legal frameworks, such as consumer protection law for example. See *inter alia*: Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427.

99 See, ao: Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a Right to Explanation' (28 June

and 15(1)h—this right broadens the attempt of Directive 95/46's Article 12(a)3rd indent to provide data subjects with the opportunity to decipher and understand the way automated decisions are made. As far as the right of access is concerned, Article 15(1)h of the GDPR encompasses the possibility for data subjects to know about the existence of automated decision-making, their logic, their significance, and their envisaged consequences. Although welcome in light of the growing use of these algorithmic systems in modern society, some have denounced the feasibility, or indeed existence of such a right to explanation. In an extensively documented paper,[100] Wachter et al. firmly criticize the wording of Article 15(1)h for lacking a clear and explicit reference to a right to obtain *ex post* explanations on the reaching of specific decisions. According to the authors, the GDPR would instead only grant data subjects a right to be informed about the general functioning of algorithmic systems, leaving the individual circumstances that have led to the making of a specific decision outside the scope of Article 15. In other words, the regulation could have gone further. Others have highlighted the restrictive definition given to the notion of 'automated decision-making'[101] which forms the basis of Article 15(1)h.[102] As a consequence, should any human take part in the process, the decision would *stricto sensu* no longer be considered as being solely based on automated processing and would not be covered by the right of access in the sense of point (h).[103] Sidestepping the GDPR would therefore prove relatively easy for reluctant controllers. These issues set aside, we believe that a teleological reading of the GDPR does imply data subjects should have the ability to obtain from controllers simple explanations as to the rationale and methodology regarding the processing of their personal data.[104] Enforcement (by DPAs and courts) and self-/co-regulatory efforts (eg standardization) will no doubt have an important role to play in how this prerogative will be operationalized in practice.

Data protection officer. As mentioned before, the empirical study laid bare a worrisome lack of awareness among controllers as to the existence and scope of the right of access. This was often due to the absence of a person in charge of dealing with privacy and data protection issues, which in turn could sometimes (though not always) be explained by the modest size of the company. Directive 95/46 left it up to Member States to define the circumstances in which the appointment of a personal data protection officer (DPO) is necessary and remained vague on its actual tasks.[105] The GDPR in contrast, clearly regulates the designation, position, and tasks of the DPO who is entrusted with an advisory, monitoring, and intermediary function.[106] Compared to Directive 95/46, the GDPR also details a series of situations in which the designation of a DPO is mandatory, while leaving it up to Member States to complete that list.[107] As far as access is concerned, the GDPR therefore brings welcome clarifications. Firstly, the DPO's extensive advisory role is likely to foster controllers' compliance with data protection rules and, therefore, positively influence the way they handle access

2016), <https://arxiv.org/abs/1606.08813> accessed 8 February 2018); Ethan Chiel, 'EU citizens might get a "right to explanation" about the decisions algorithms make' *Splinternews* (7 May 2016) <https://splinternews.com/eu-citizens-might-get-a-right-to-explanation-about-the-1793859992> accessed 8 February 2018; Aviva Rutkin, 'Interrogating the algorithms', *NewScientist* (16 July 2016) 19; Joon Ian Wong, 'The UK Could Become a Leader in AI Ethics – If This EU Data Law Survives Brexit', *Quartz Blog* (12 October 2016) <https://qz.com/807303/uk-parliament-ai-and-robotics-report-brexit-could-affect-eu-gdpr-right-to-explanation-law/> accessed 8 February 2018); Edwards, Lilian and Michael Veale. 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (23 May 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855> accessed 8 February 2018; Christopher Kuner, , and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 7 International Data Privacy Law 1; Fink, Katherine, 'Opening the Government's Black Boxes: Freedom of Information and Algorithmic Accountability' (2017) Information, Communication & Society 1–19. doi:10.1080/1369118X.2017.1330418.

100 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 and also <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469> accessed 8 February 2018.

101 Defined by art 22(1) GDPR as a decision based *solely* on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her (emphasis added).

102 Lee A Bygrave, 'Automated Profiling: Mind the Machine. Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law and Security Review 20, especially condition 3; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in J Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press, Amsterdam, Washington DC 2012) 51. She specifically points out that 'as soon as the decision is not automated due to a (routine) human intervention, the article [22 GDPR] no longer applies'.

103 Chiel (n 99).

104 See also: Art 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 63).

105 For an overview of the national legislation echoing that possibility, see: Confederation of European Data Protection Organisations, 'Comparative analysis of data protection officials' role and status in the EU and more' <https://www.afcdp.net/IMG/pdf/European_DPO_Comparative_Analysis_6-feb-2012_AFCDP_CEDPO.pdf> accessed 8 February 2018.

106 See on these specific points: Arts 37–39 of the GDPR.

107 For more information on the designation, position and roles of the data protection officer under the GDPR, see: Paul Lambert, *The Data Protection Officer: Profession, Rules, and Role* (CRC Press, London, New York 2016); Stefano Varotto and Colin James, 'The European General Data Protection Regulation and its potential impact on businesses: Some Critical Notes on the Strengthened Regime of Accountability and the New Sanctions' (2015) Communication Law 81–82.

requests. Data subjects in turn, may expect more expertise in the answers they receive. Secondly, controllers are obliged to publish the contact details of their officer, while data subjects are explicitly granted the possibility to contact the latter with regard to all issues related to the exercise of their rights.[108] This should greatly help prevent the troubles related to identifying and locating the appropriate contact point to send requests to (above, the sub-Section 'Is there still a role for data subject empowerment?'). It remains to be seen how especially SMEs will deal with potentially extra rules imposed at the Member State level.

Data protection by design and by default. Whereas Directive 95/46 simply obliged controllers to ensure compliance with the general principles governing the processing of personal data,[109] the GDPR introduces a specific duty to implement appropriate technical and organizational measures to that end (Article 25). This provision titled 'data protection by design and by default',[110] requires controllers to adopt a proactive attitude towards data protection issues by embedding privacy-conscious features into the architecture of their IT systems themselves, and at every step of their processing activities. Combined with the focus on 'accountability' (Article 5(2)) this approach should eventually become organizations' default mode of operation. Controllers could, for example, implement machine-readable privacy policies that would facilitate data subjects' understanding of complex legal issues and enable a more scalable management of one's privacy preferences.[111] On top of that, they will have to profoundly reconsider how they collect, store, and process personal data, an exercise which is likely to require deep collaboration between different departments. In doing so, controllers could be forced to review their IT systems and revamp their indexation and storage methods to ensure proper compliance with data protection general principles and a better handling of access requests (and other data subject rights). The European Data Protection Supervisor has also encouraged developers to come up with new and innovative ways for data subjects to exercise control over their data.[112] In any case, data protection by design undoubtedly appears as a step in the right direction when it comes to strengthening data subjects' informational empowerment.[113] However, as was mentioned above, making it harder and/or complex to retrieve personal data on an individual basis could be seen as a data protection by design measure, but it cannot justify controllers refusing to accommodate data subject rights altogether.

Accountability. The accountability principle introduced by Articles 5(2) and 24 of the GDPR requires companies to take appropriate technical and organizational measures to ensure a proper implementation of data protection principles, and, above all, to be able to demonstrate compliance upon request. This is likely to place a heavier burden on controllers who will have to determine the nature and scope of the measures to be carried out on their own, while simultaneously facing the risk of serious fines (see Articles 79, 82 and 83 GDPR).[114] To the extent the accountability principle will actually make true on its promise of foster controllers' compliance with data protection rules, it also implies an improvement for how data subject rights will be accommodated.

Codes of conduct and certification mechanisms. The GDPR introduced several provisions aimed at (facilitating) translating abstract rules to more concrete, practice oriented situations.[115] Article 40, for example, builds on a concept that was already included in Directive 95/46 but had received little to no attention at the time.[116] It

108 Respectively arts 37(7) and 38, 64 of the GDPR.

109 Art 6(2) of the Directive 95/46.

110 The term can be traced back to the concept of 'privacy by design', generally ascribed to Ann Cavoukian. See for instance: Resolution on Privacy by Design, adopted during the 32 International Conference of Data Protection and Privacy Commissioners in Jerusalem (27–29 October 2010) <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> accessed 8 February 2018. For more information on the impact of the Resolution, see: Ontario Information and Privacy Commissioners' report on the state of Privacy by Design to the 33rd International Conference of Data Protection and Privacy Commissioners', 'Privacy by Design. Strong Privacy Protection - Now, and Well into the Future' <https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf> accessed 8 February 2018.

111 See for example the Platform for Privacy Preferences (p3p) project, which has developed a method for websites to compile their privacy practices in a standard format that can be retrieved automatically and interpreted by user agents <https://www.w3.org/P3P/> accessed 8 February 2018. See also: Inger Anne Tøndel and Åsmund Ahlmann Nyre, 'Towards a Similarity Metric for Comparing Machine-Readable Privacy Policies' in Jan Camenisch and Dogan Kesdogan (eds), *Open Problems in Network Security* (Springer, Berlin, New York 2011) 89–103; LF Cranor, 'Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2012) 10 Journal on Telecommunications and High Technology Law 273–307; Lehtiniemiand Kortseniemi (n 75) 1–11.

112 European Data Protection Supervisor, 'Opinion 7/2015: Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability' (19 November 2015) 14 <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 8 February 2018.

113 Varotto and James (n 108) 79.

114 On the new criminal penalties, administrative fines and class action claims: Ibid 81–82.

115 The WP29 had already stressed the need to avoid a uniform approach toward different processing activities in its Opinion 3/2010 on the principle of accountability: Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (13 July 2010) 13, s 45 <https://ec.europa.eu> accessed 8 February 2018.

116 Art 27 Directive 95/46. However, no significant initiative has been taken to date: Paul de Hert and Vagelis Papakonstantinou, 'The new General

allows associations or other bodies representing categories of controllers or processors to prepare codes of conduct intended to contribute to the proper application of, among others, the exercise of the various rights granted to data subjects.[117] Controllers can therefore benefit from adequate, more fine-tuned guidance on how they should apply the new text in light of the nature and scope of their own activities. Similarly to codes of conduct, certification mechanisms are aimed at bridging theory and practice in the GDPR. Whereas the main added value of codes of conduct is to translate abstract rules to specific contexts/sectors, certification mechanisms' worth lies in making GDPR compliance enforcement more scalable. Articles 41–42 encourage the establishment of recognized certification mechanisms, seals and marks, at national or EU level, aimed at providing suitable guidance and helping controllers to demonstrate their compliance with data protection rules.[118] In light of their ambitions, both codes of conduct and certification mechanisms will potentially foster a better understanding of, and adherence to, data subject rights by controllers. Yet, looking at how similar instruments have worked in other sectors (eg financial industry), some scepticism as to their added value seems warranted.[119]

Data protection authorities and the European data protection board. Member State DPAs play a key role when it comes to the practical implementation of the right of access within their jurisdiction.[120] The wide margin of appreciation left to Member States under Directive 95/46 has prevented the development of a uniform approach on how to handle access requests.[121] The GDPR introduces new mechanisms to foster a more consistent decision-making process among national DPAs such as a 'one-stop-shop' procedure and a consistency mechanism.[122] Still quite broad and untested, these provisions at least have the potential to contribute to a more harmonized—and therefore arguably more forceful—interpretation and enforcement of the right of access across the EU.[123] In addition to their monitoring and enforcement role, DPAs are also entrusted with a task to raise awareness on rights and obligations in the GDPR.[124] So far, many DPAs seem to already provide guidance on how data subjects should exercise their right of access and how controllers should accommodate such requests.[125] An even more proactive stance by DPAs, eg advocating and/or provide tools to intermediate access requests, would greatly help tackle many of the issues identified in the Section 'The future. A new era for data subject rights?'. Finally, it is also worth highlighting the new European Data Protection Board (EDPB), whose mission and powers considerably extend beyond those of its predecessor, the WP29. The EDPB's role vis-à-vis the right of access will primarily be through its involvement in developing and/or verifying guidelines, codes of conduct and certification mechanisms (above).[126]

Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law and Security Review 192, especially point 13.

117 See notably art 41(2)f of the GDPR which deals with data subject's rights. For the full list of areas that may be covered by codes of conduct, see art 40(2)a-k.

118 On top of serving as basis to demonstrate compliance with the GDPR as required by the accountability principle (art 24(3)), certification mechanisms may also: demonstrate compliance with the data protection by design and by default principles (art 25(3)), demonstrate the sufficient guarantees offered by processors (art 28(5)), demonstrate compliance with the security requirements (art 32(3)) provide appropriate safeguards in case of transfers of personal data to third countries (arts 40(2), 46(2)f) and influence the determination if potential fines (art 83(2)j). This generally follows the same logic as for codes of conduct.

119 To be fair, arts 41 and 43 do aim to clearly delineate the scope of bodies monitoring codes of conduct and/or certification.

120 They are indeed entrusted with the task of monitoring and enforcing the provisions laid down in data protection legislation and hear individuals' complaints, mediate between data subjects and controllers and take binding decisions like judicial authorities would do in first instance. See: Art 28(1) and (4) of the Directive 95/46 and art 57(1)a of the GDPR. See also: Galetta and de Hert (n 29) 38–40, point 3.9.

121 See for example: European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II' (2010) <http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities> accessed 8 February 2018. The empirical study conducted in the context of the IRISS project has pointed out worrying fluctuations in DPAs efficiency due to a lack of resources: Clive Norris and L'Hoiry (n 52) 453–54; Antonella Galetta and others, (n 23) 472–74.

122 For the 'one-stop-shop' procedure, see art 56 GDPR. The WP29 has also recently issued its Guidelines for identifying a controller or processor's lead supervisory authority, adopted on 13 December 2016, WP244. See also: Galetta and de Hert (n 36) 144. For the consistency mechanism, see art 64(2) of the GDPR. It is worth noting that the consistency mechanism was mainly introduced to ensure uniform application of decisions taken by national supervisory authorities that produce effect in more than one Member State.

123 See European Commission, 'The Proposed General Data Protection Regulation: The Consistency Mechanism Explained', available at the address www.ec.europa.eu (accessed on Friday, 11 August 2017).

124 Compared to Directive 95/46 which left details up to Member States, the GDPR clearly highlights their advisory functions and dedicates a series of provisions to that end. See, arts 57(1)b, d-g and I, and art 58(3)b of the GDPR.

125 See for example: the British Information Commissioner's Office's (ICO) 'Guide to Data Protection' that dedicates a section to subject access request <https://ico.org.uk/for-organisations/guide-to-data-protection/> accessed 8 February 2018; the French Commission Nationale de l'Informatique et des Libertés's (CNIL) guidelines on the right of access <https://www.cnil.fr/fr/le-droit-dacces> accessed 8 February 2018; the Belgian Commission Vie Privée's guidance on how to exercise the right of access as a data subject <https://www.privacycommission.be/fr/exercice-droit-acces> accessed 8 February 2018; and the Dutch Autoriteit Persoonsgegevens' page on the right of access <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-inzage?qa=inzage>accessed 8 February 2018.

126 For the EDPB's advisory role, see art 70(1)e and the list of areas in which these recommendations could be necessary in point f to m. For the

Beyond the GDPR, beyond the legal framework. Zooming even further out, the right of access can and is improved through elements that do not emanate from the law *stricto sensu*. Technological tools are playing an increasing role in making the right of access easier to accommodate *and* exercise, but also help in raising general awareness on information asymmetries and empowering data subjects. Indeed, this is exactly the motivation behind civil society initiatives such as Bits of Freedom's PIM tool[127] and AccessMyInfo[128] for example.[129] Similarly, a whole community of developers is emerging specifically focusing on new business models based on facilitating access requests, both from controllers'[130] as well as from data subjects' perspective.[131] Collective action—through DPAs, consumer protection organizations, or grass-roots initiatives—are also bound to play an important role in emboldening data subjects (above).[132]

Conclusion

The right of access has always played a central role in data protection law. It was the first important data subject empowerment tool and can be seen as a necessary enabler for most other data subject rights. The right can also play an important role in monitoring operations and (en)forcing compliance. Despite some high-profile revelations regarding unsavoury data processing practices over the past few years, access rights still appear to be underused and not properly accommodated. It is especially this last hypothesis we tried to investigate and substantiate through a legal empirical study. During the first half of 2017, around 60 information society service providers were contacted with data subject access requests. The different steps, interactions and overall findings were gathered through formalized questionnaires by advanced master students in law. This allowed empirical evaluation of (i) privacy policies; (ii) the actual filing of an access request; (iii) correspondence with controllers; and (iv) responses given to access requests. Eventually, the empirical study confirmed the general suspicion that access rights are by and large not adequately accommodated. The systematic approach did allow for a more granular identification of key issues and broader problematic trends. Notably, it uncovered an often-flagrant lack of awareness (of the scope and extent of data protection rules); organization (both technically and organizationally); motivation; and harmonization. Indeed, the study demonstrated that the already low number of companies deeming themselves 'compliant in terms of individuals' data protection rights' (24 per cent),[133] may be undeservedly over-confident.

Drawing on these observations, the final section of this contribution looked ahead, at how the GDPR may (not) improve the current status quo and if there is still a role for data subject empowerment tools in the first place. With regard to the latter, it was concluded that data subject empowerment (or control) still has a crucial and underestimated role in a hyper-complex, automated and ubiquitous data-processing ecosystem. Even if only used marginally, they provide a checks and balances infrastructure overseeing controllers' processing operations, both on an individual basis as well as collectively. The empirical findings also allow identifying concrete suggestions aimed at controllers, such as relatively easy fixes in privacy policies and access rights templates. Eventually, this article places the right of access against the broader backdrop of the GDPR, its many interacting provisions and how they (do not) contribute to a more effective right of access.

In sum, the purpose of this article is to lift the veil on how the right of access is actually (not) accommodated by information society service providers. Indeed, the underlying empirical study effectively made it possible to pinpoint core issues and challenges faced by data subjects exercising their rights in practice. This, in turn, effectively enables a properly informed debate among all stakeholders in the search for better policy, enforcement, and compliance strategies. After all, data protection law and the values it aims to protect, are but an illusion when assessed through a one-way mirror.

doi:10.1093/idpl/ipy001

EDPB's role in the consistency mechanism, see: art 65(1) and (2). See also n 133 for a more comprehensive comment and Bridget Treacy, Adam Smith, 'The European Data Protection Board – More than a mere rebranding exercise' (2016) 16 Privacy and Data Protection 11–12. For the EDBP's role in the elaboration of codes of conducts, see: arts 40(1), (7), (11) and 70(1)n, x.

127 <https://pim.bof.nl>.

128 <https://accessmyinfo.org/>. This tool is addressed at Canadian citizens.

129 See also above, the sub-Section 'Filing access requests'.

130 For example: OneTrust's Data Subject Access Request Portal, <https://onetrust.com/onetrust-launches-first-market-data-subject-access-request-dsar-portal-simplify-gdpr-compliance/>.

131 See notably the mydata.org community. Hae.datam.me or Personaldata.io, for example, aim to automate all the often-necessary interactions with controllers in order to obtain an adequate response from controllers.

132 Wim Nauwelaerts, 'Practitioner's Corner · GDPR - The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer' (2017) 3 European Data Protection Law Review 251, 254–56.

133 Ibid 254.