The London School of Economics and Political Science

THE INDIVIDUAL IN EU DATA PROTECTION LAW

Katherine Anne Nolan

A thesis submitted to the Department of Law of the London School of Economics and Political Science for the degree of Doctor of Philosophy, London, 16 March 2023

DECLARATION

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

I declare that my thesis consists of 98,147 words.

ABSTRACT

The individual and the idea of the individual are at the centre of EU data protection law, particularly the General Data Protection Regulation ("GDPR") and the fundamental right to data protection under Article 8 of the Charter of the Fundamental Rights of the European Union. Critiques of that role have emerged, and exist in parallel to broader concerns about individualist tendencies of information privacy law. These concerns go to the heart of the law's capacity to protect individuals and groups, and to ensure a just digital society, and the understanding of what data protection law sets out to achieve.

I argue that an understanding of the role and conception of the individual is central to understanding EU data protection law, both its promise and limitations. The individual's role in the GDPR emerges as a multi-faceted one, at times contradictory. Understanding this role can enable us to more precisely assess the GDPR and imagine alternative regulatory approaches to data protection. Placing the role of the individual in EU data protection law in historical and institutional context helps us to see that the notion of the individual, their status and capacities, have shaped the regime, and that many of the assumptions underpinning this notion of personhood in the regime also merit question. The conception of the individual in EU data protection law is analysed according to three parameters of personhood: relational versus individuated, empowered versus protected and different versus uniform. The picture of personhood which emerges is fragmentary, and reveals ideas and assumptions which have informed the regime, which can indicate limited understandings of personhood and gaps in the reach of EU data protection law. By re-engaging with these assumptions and the multi-faceted role of the individual, new understandings of the GDPR, associated case law and the right to data protection are possible.

ACKNOWLEDGMENTS

This thesis is the culmination of many years' work, and in that time I have been incredibly lucky in the support I received from family, friends and colleagues. While I cannot truly express what this has meant to me in some short words, I do want to thank some people in particular.

My family, especially my Mum and Dad, brother Hugh and sister-in-law Caoimhe, have listened to many worries and concerns, and have probably heard more about data protection law than they ever cared to. Their company and love has be an unwavering source of comfort and support.

I am very fortunate in my friendships. The comradery, cheering on and consolation of my friends has enabled me to push on and complete this thesis, even when we were isolated from one another, first by distance and then by a global pandemic. Especially, and in no particular order, I want to thank Úna Kelly, Liz Burke, Lauren Alexander, Emma Lawrence, Emer Ní Chúagáin, Aislinn O'Toole, Máiread Nic Gabhann, Charlotte Cooper-Davis, Jack Cleary, John O'Brien, Andrea Mulligan, Bláithín Ní Chróinín, Janis Wong, and Sahar Ahmed for their friendship.

In the LSE Law School I received excellent support in the completion of this thesis. My supervisors, Prof. Andrew Murray and Dr. Orla Lynskey, were from the beginning of the journey excellent supervisors, always pushing me to be a better scholar, while helping me navigate through the rougher patches. I am so grateful for their mentorship and encouragement.

I was also lucky to meet a variety of interesting researchers at the LSE, with whom I had many fruitful and challenging discussions, and some of whom have become friends over the years, including: Stephanie Classmann, MacKenzie Common, Alexandra Sinclair, Mattia Pinto, Francesca Uberti, Carly Krakow, Rachna Matabudul, Viknes Muthiah, Ben Goh, Parashar Das, Fletch Williams, Fatima Ahdash, Giulia Gentile, Valerie Verdoodt, and Malavika Raghavan. I would also like to offer special thanks to Dr. Stephen Humphreys and Dr. Andrew Scott who acted as my first year upgrade reviewers, and provided valuable feedback on my project at an early stage. I also wish to thank Dr. Sarah Trotter and Prof. Susan Marks for helpful guidance and conversations in the first year of my PhD.

Aspects of this thesis have been presented or discussed elsewhere, and I wish to acknowledge the valuable feedback and suggestions I have received in a number of fora, particularly from the commentators at the Society of Legal Scholars Annual Conferences 2020 and 2021, at BILETA Annual Conferences 2021 and 2022, CPDP 2022 and the Law, Tech and Theory Seminar at the University of Helsinki in February 2023. I received helpful suggestions from a number of scholars, but I would like to especially thank Prof. Paul Schwartz, Dr. Eoin O'Dell, Dr. David Fennelly, Prof. Arno Lodder, Prof. Gloría Gonzalez Fuster, Dr. Edina Harbinja, Prof. David Erdos and Prof. Susanna Lindroos-Hovinheimo for engaging with my work and challenging me to make it better.

Finally, I wish to acknowledge that part of Chapter 2 will be published in 'The multi-faceted role of the individual in data protection law' (Matsumi, Hallinan, Dimitrova, Kosta and de Hert (eds) *Data Protection and Privacy, Volume 15: In Transitional Times* (2023 Hart Publishing)).

TABLE OF CONTENTS

INTRODUCTION

In this thesis, I advance the argument that the individual is central to EU data protection law, particularly the General Data Protection Regulation ("GDPR")[1] and the fundamental right to data protection as protected by Article 8 of the Charter of the Fundamental Rights of the European Union (the "Charter"). The individual's role emerges as a multi-faceted one, and these facets are not always consistent with one another. The protection of the individual and their right to the protection of personal data is the primary goal of the GDPR. In order to achieve this protection, the threshold of application of the GDPR is defined in terms of the individual through the concept of personal data. Assessment of the legality of processing is closely tied to an assessment of the impact on an individual's interest. The individual is armed with rights to protect their own interests against data controllers, and to secure redress where their rights are infringed. While we cannot say the GDPR is entirely individualistic, the individual and their interest are central to the framing and operation of the regime.

Because of the centrality of the individual, it is a valuable parameter against which to question EU data protection law and the GDPR. When we assess the role of the individual in the GDPR, a number of limitations emerge, including the possibility of under-inclusiveness, scaling up the enforcement burden of EU data protection law by individualising complaints, and improper responsibilisation of individual data subjects as defenders of their own interests.

To understand why the individual takes such a central role in the GDPR, the role of the individual should be placed in context. I argue that the role of the individual can be understood at least partially by reference to certain historical and institutional context. By considering that the individual's role can be associated with the emergence of European fundamental rights protections and the European Union project, we can recognise that the role in which we place the individual is a product of various traditions and political positions. Current legal approaches are thus not inevitable. Once viewed in this light, we can see that the role in which we place the individual is in part a result of conceptions of personhood, as assumptions about the individual and their place inform the regulatory choices underpinning EU data protection law.

By opening up questions of personhood, we can ask how conceptions of the individual underpin EU data protection law. Three parameters of personhood are considered, to deepen our understanding of the regime, and the assumptions which ground it. Engaging with relationality of personhood, we see that the individuated[2] model of personhood creates challenges in the regulation of plural personal data sets. Looking to the balance between empowerment of the individual and paternalism, a marketized vision of empowerment appears, as do questions as to what a coherent normative account of what a paternalistic

---

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4/5/2016, p 1–88).

[2] By individuation, I mean the distinction and separation of persons from one another as individuals. EJ Lowe, 'Individuation' in Michael J Loux and Dean W Zimmerman (eds), *The Oxford Handbook of Metaphysics* (Oxford University Press 2005) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199284221.001.0001/oxfordhb-9780199284221-e-4> accessed 25 September 2019.

strategy of protection should entail. Finally, by looking to the manner in which persons are assumed to be homogenous versus different, a fractured picture emerges. Some express differences are recognised and protected, and individualised standards of protection allow for some differentiation according to circumstance, but others are excluded entirely from the regime due to assumptions regarding capacity.

These questions and the tensions which emerge go to the heart of EU data protection law, and thus understanding the role and conception of the individual contributes to our understanding of EU data protection law, its possibilities and its limitations.

1. Object of study and approach

In this section I introduce the aspects of EU data protection law which are the focus of this thesis and the approach and methodology I have taken.

1.1. The core of EU data protection law: Article 8 of the Charter and the GDPR

This thesis, in referring to EU data protection law, is primarily concerned in particular with Article 8 of the Charter, which protects the right to data protection, and the legislation which gives expression to that right,[3] the GDPR, as well as its predecessor the Data Protection Directive.[4] Where the right to data protection or the relevant legislation have been interpreted through the case law of the Court of Justice of the European Union ("CJEU") this also forms part of this study. Other legislative instruments (such as the Law Enforcement Directive,[5] the ePrivacy Directive[6] and Regulation 2018/1725[7]) which adopt sectoral specific data protection measures are not the central focus of this thesis. Rather I focus on the core of generally applicable data protection which I locate in Article 8 and the GDPR.

The European Convention on Human Rights (ECHR) is also a significant source of EU data protection law, particularly due to the connection between Article 8 of the ECHR, which protects the right to respect for private life, and Articles 7 and Article 8 of the Charter. The Charter confirms that fundamental rights which have corresponding rights to those under the

---

[3] See discussions in Elise Muir, 'Of Ages In-and Edges Of-EU Law' (2011) 48 Common Market Law Review 39; Elise Muir, 'The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges' (2014) 51 Common Law Market Review 219. See also Case C-154.21 *RW v Österreichische Post AG* (ECLI:EU:C:2023:3), para 44 which provides in part "the general legal framework created by the GDPR implements the requirements arising from the fundamental right, protected by Article 8 of the Charter of Fundamental Rights of the European Union, to the protection of personal data, in particular the requirements expressly laid down in Article 8(2) thereof."

[4] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995, p 31–50).

[5] DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4/5/2016, p 89-131).

[6] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/7/2002, p 37–47) 200.

[7] REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21/11/2018, p.39-98).

ECHR should be interpreted the same, though the EU can provide a higher level of protection.[8] While this thesis does not provide a systematic analysis of all of the case law of the European Court of Human Rights ("ECtHR") which concerns the individual in data protection,[9] the thesis does draw on the ECHR and decisions of the ECtHR where relevant to the assertion of the right to data protection by the individual, to the interpretation of Article 8 of the Charter, and to compare and contrast notable conceptions of personhood evident in the decisions of the ECtHR to those found in decisions of the CJEU or in EU legislation.

1.2. Methods: approach

The research question which this thesis responds to is "What is the role and conception of the individual within EU data protection law, and what is the significance of this role and conception for EU data protection law?"

The Data Protection Directive, by its title, sets out to achieve "the protection of *individuals* with regard to the processing of personal data,"[10] which in the GDPR has been replaced with references to the protection of "natural persons". Moreover, the Charter proclaims that the European Union "places the individual at the heart of its activities".[11] The concept of the "individual" offers us a particular way in which to think about the natural person, a construct of an autonomous, individuated person endowed with dignity and agency,[12] ideas which find representation in the EU data protection regime. I contend both the role and conception of the individual have significance to EU data protection law.

With the element of the "role" of the individual, this PhD begins with a concern about legal doctrine: what is the legal significance of the status of the individual in EU data protection law? I use "role" in this way to refer to the technical, legal place that the individual takes.[13] It is in light of this legal significance that I consider the role of the individual, and construct an understanding of the individual. The approach to this question, begins with a doctrinal enquiry, by way of a review of the legislative instruments, case law of the CJEU, and regulatory guidance.[14] A conceptual model of the individual is constructed based on an inductive review of these materials.[15] My understanding and normative analysis of these

---

[8] Article 52(3), of the Charter provides: "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

[9] This is reserved for future work.

[10] Data Protection Directive. (My emphasis.)

[11] Charter, Preamble.

[12] Often associated with a liberal theory of law or human rights, though with precursors in earlier religious and humanist traditions. See Costas Douzinas, *The End of Human Rights: Critical Thought at the Turn of the Century* (Bloomsbury Publishing Plc 2000); Alexander Somek, *Individualism: An Essay on the Authority of the European Union* (Oxford University Press 2008); Larry Siedentop, *Inventing the Individual: The Origins of Western Liberalism* (Penguin Books 2014); Catherine Dupré, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Bloomsbury Publishing Plc 2015); Sarah Jane Trotter, 'On Coming to Terms: How European Human Rights Law Imagines the Human Condition' (Doctor of Philosophy, The London School of Economics and Political Science 2018) <http://etheses.lse.ac.uk/3946/1/Trotter__On-coming-terms-European-human-rights.pdf>.

[13] See Brożek who points to the use of the notion of the person having "technical (legal) character." Bartosz Brożek, 'The Troublesome "Person"' in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017) 9.

[14] See further, section 1.3 below.

[15] For a more in-depth description of the method by which my conceptual model of the individual is made, see Chapter 2, section 1.1.

legal texts is supported by my engagement with the overlapping academic literatures of data protection, privacy and surveillance studies scholarship. The surveillance studies literature has been particularly helpful in grounding my ideas and understanding of the environment in which EU data protection law exists and to which it contributes.

In this thesis, I argue that an analysis of only this formal role of the individual is incomplete, and therefore I differentiate between the role and the conception of the individual. When I refer to these "conceptions" of the individual, I am considering the abstracted individual who is represented in the legal regime,[16] and asking how is such an individual understood and represented? As Boyle puts it, "[t]he subject is loaded up, consciously or unconsciously, with a particular set of qualities or attributes. That subject then reflexively produces a kind of society, a legal decision, or a professional practice."[17] Interested in these assumed qualities and attributes of personhood, the second half of this thesis engages with how particular conceptions of personhood are found within EU data protection law. The enquiry is still primarily concerned with analysis and interrogation of the legal texts, but the focus deepens, as I look to how ideas of personhood and individuality inform the structure and operation of EU data protection law. Given the myriad constructions of personhood available, a comprehensive account is not the ambition of this thesis. Rather, I draw on three key parameters of personhood: relationality versus individuation, empowerment versus paternalism and difference versus uniformity. Each of these parameters are signalled expressly in the case law and legislative framework, which inspired their choice, and also allow us to bring our discussion into conversation with wider literatures on legal personhood.

Ideas of personhood are not merely of theoretical interest, they shape the operation of the law.[18] This examination of how the individual is represented in the EU framework allows us to reveal a series of insights about underlying assumptions and pre-suppositions.[19] In constructing conceptions of personhood against which to measure the legal texts, I also rely on literature concerning legal personhood, particularly legal personhood within the EU context. This adds a conceptual piece to the thesis, where legal doctrinal analysis is complemented with a theoretical consideration of the ways in which the legal regime embodies particular notions of the individual.

Additionally, in choosing to engage with the richness and detail of the legislative framework in its entirety, rather than isolated provisions or principles, a certain degree of complexity is

---

[16] As Naffine has written, when we speak of the legal subject, we can be comfortable with the idea that this subject is a legal fiction, an abstraction. Ngaire Naffine, 'Legal Persons as Abstractions: The Extrapolation of Persons from the Male Case' in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017).

[17] James Boyle, 'Is Subjectivity Possible - The Post-Modern Subject in Legal Theory' (1991) 62 University of Colorado Law Review 489, 518.

[18] See Chapters 3, 4, 5 and 6. A number of scholars have observed how our ideas/definitions of the person have concrete effect in the world, including through law. Brożek (n 13) 15; Naffine (n 16) 24. Charlotte O'Brien, 'I Trade, Therefore I Am: Legal Personhood in the European Union' (2013) 50 Common Market Law Review 1643, 1645. More broadly, Bygrave has observed that "[t]he way in which one conceptualises the interests and values served by these laws is not just of academic interest but has significant regulatory implications." Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) 7.

[19] On this, I take inspiration from Lindroos-Hovinheimo, whose "analysis of legal personhood attempts to reveal its ideological embeddedness." Susanna Lindroos-Hovinheimo, 'Private Selves - An Analysis of Legal Individualism' in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer International Publishing 2017) 30. See also Boyle (n 17).

inherent to this thesis. Rather than responding to a model of data protection law which is abstracted, or trying to rationalise all aspects of EU data protection law into a single coherent narrative, I am attempting in this thesis to embrace its complexity, even where EU data protection law can tend towards the labyrinthine.

1.3. Methods: sources and limitations

While this thesis seeks to offer a more detailed account of the role and conception of the individual in EU data protection law than found in existing scholarship, there are necessary limitations to the account in accordance with choices made as to the methods, to sources relied upon and to the scope of the thesis.

First, in relation to the legal sources relied upon, the primary emphasis is upon law as it manifests in EU legislation and the decisions of the CJEU. Insofar as EU legislation is relied upon to construct the account in this thesis, the majority of the analysis is founded on the final legislative text adopted. Some of the relevant legislative history has been drawn upon in part in considering some of the historical connections of relevance to the thesis,[20] but this history does not purport to be exhaustive. To the extent that the analysis in this thesis represents the position or intent of legislators (either national or EU legislators) or of the CJEU, this is in an abstracted sense, drawn from the position manifested in the final legislation or decisions of the CJEU. While competing viewpoints and perspectives are no doubt present as between different components of the EU legislator or different members of the judiciary on data protection matters, this thesis does not attempt to map such perspectives. Further, both the operative text and recitals of the relevant EU legislation are drawn upon in constructing my account of the individual. It should be acknowledged that the recitals to EU legislation are non-binding as a matter of law.[21] Nevertheless, the recitals have an important role in guiding legal interpretation of operative text, and therefore can contribute to our understanding of EU legislation.[22] It is in this interpretative sense that I rely upon legislative recitals in this thesis. When it comes to reliance upon decisions by the ECtHR, a selective approach has been adopted where leading relevant cases are analysed to illustrate areas of commonality or contrast, but this thesis does not purport to be comprehensive as to the role or conception of the individual before the ECtHR.

Second, in relation to academic literature drawn upon, while all efforts have been made to incorporate relevant literature such is available in the English language, this necessarily excludes relevant materials published in other languages. This choice was made by necessity, due to the author's lack of fluency in other relevant languages.

Finally, the content of this thesis (and underlying legal and academic sources) was up to date as of the original submission date of 16 March 2023.

As a result of such choices made, the thesis has associated limitations. While the thesis seeks to contribute a more detailed account and problematisation of the role and conception of the individual in EU data protection law than previously found in the literature, it cannot claim to be exhaustively comprehensive. The account is primarily legal. The legal sources drawn upon are mainly EU legislation, cases of the CJEU, and selected leading cases of the

---

[20] See Chapter 3.

[21] See e.g. Case 215/88 *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung* (ECLI:EU:C:1989:331), para 31: "Whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule."

[22] Tadas Klimas and Jflrate Vaitiukait, 'The Law of Recitals in European Community Legislation' (2008) 15 Journal of International & Comparative Law 60; Llio Humphreys and others, 'Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation' [2015] JURIX 41.

ECtHR, and thus the account of "EU data protection law" is in this sense.[23] The representation of the EU, the "EU legislator" and the CJEU in an abstracted manner is reductive in the sense that it eliminates the complexity of differing factions and viewpoints. It can be useful analytically to represent this unified position, at least as a starting point, as to the position that manifests in the final legislation or judicial decisions. Nevertheless it should be read as such, as a starting point.[24] Further, the understanding of the relevant legislation is guided by reliance upon the recitals to that legislation in an interpretative sense, as mentioned above. However, there is a degree of uncertainty in so relying upon the recitals due to their non-binding status. Additionally, given that there is not a systematic mapping of all ECtHR decisions addressing data protection, this thesis cannot be exhaustive as to the role and conception of the individual before the ECtHR, but rather observes some of the key aspects of the jurisprudence by way of comparison to approaches of the CJEU or found in the GDPR. Future work might build upon this thesis to look to other relevant sources, to expand the comprehensiveness of the account of the role and conception of the individual in EU data protection law.

Additionally, an exhaustive historical account of the role of the individual is not attempted in this project, and therefore it cannot claim to be so. In Chapter 3, where the primary historical contextualisation of the thesis is contained, a further explanation is found as to the aims and limitations of that account.[25]

Further, as thesis has been constructed through reliance upon English language sources, there are inevitably relevant theories, sources and works in other languages which unfortunately have not contributed to this account. Therefore, this thesis should be understood in this regard and does not claim to be comprehensive as to all relevant academic theories or commentary.

2. Contextualising data protection

Doubts exist whether the GDPR is capable of meeting its self-described mission, to ensure that "[t]he processing of personal data should be designed to serve mankind".[26] As we shall see, many of these doubts arise due to a perceived mismatch between EU data protection law and the environment in which it operates. Of course, it is simplistic to characterise the law as merely responding to an environment, the law and legal institutions are a part of the environment, dynamically interacting with and shaping actors and behaviours.[27] In this thesis, therefore, I ask not only how EU data protection law responds, but also how it contributes to its environment. Therefore, a contextualisation of EU data protection law and brief exploration of the forces driving data processing is worthwhile. The GDPR itself points to "a substantial increase in cross-border flows of personal data",[28] while the "scale of the collection and sharing of personal data has increased significantly".[29] Two interconnected forces in particular have contributed to such an increase in scale, and beyond mere quantum

[23] Consideration of how these sources have been implemented in domestic legal regimes is reserved for future work.
[24] Future work could delve into the tensions between different constituent elements of the EU legislator or other actors as to the role and conception of the individual.
[25] See Chapter 3, section 1.
[26] Recital 4, GDPR.
[27] The nature of this interactive mechanism is a matter of debate which is beyond the scope of this thesis, but see for example Chris Reed and Andrew Murray, *Rethinking the Jurisprudence of Cyberspace* (Edward Elgar Publishing 2018) 139–167; Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[28] Recital 5, GDPR.
[29] Recital 6, GDPR.

of data processing, shaped the nature of data collected and the incentives for data processing. These forces are those of datafication and informational capitalism.

Datafication refers to the translation of a phenomenon into a quantified format so that it can be tabulated and analysed.[30] In other words, something is rendered into data and therefore may be subjected to an array of modern data analysis techniques. The belief in the superiority of big data analytics[31] has driven the push for greater datafication. As Mejias and Couldry have written, datafication is a transformative process—"a process of abstraction" of the real.[32] Thus we have seen the datafication of relationships, experiences, moods through social networking,[33] and the deployment of tracking and identification technologies such as cookies, beacons and pixels to monitor individual's web and device usage, generating deeper and (notionally) more valuable individual profiles.[34] Further insights can be derived when online behavioural data is combined with offline sources of data, to generate rich profiles of behaviour.[35]

The associated economic forces which have arisen to exploit data have also shaped the environment in which data protection law applies, and the form of the legislation itself. The two best models of these phenomena are Zuboff's "surveillance capitalism" and Cohen's "informational capitalism."[36] Zuboff's focus is on particular business models which exploit data—so called "data exhaust", the behavioural data associated with customers/users and the commodification of such data.[37] Zuboff points in particular to business models, and does not object to the use of such data (or behavioural surplus) being used by organisations to improve existing goods or services, but rather to the new business uses for advertising and

---

[30] Coined by Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Mariner Books 2014) 90. See also Jose Van Dijck, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12 Surveillance & Society 197; Jens-Erik Mai, 'Big Data Privacy: The Datafication of Personal Information' (2016) 32 The Information Society 192; Ulises A Mejias and Nick Couldry, 'Datafication' (2019) 8 Internet Policy Review <https://policyreview.info/concepts/datafication> accessed 25 July 2022. Van Dijck 198.

[31] Big data may be said to refer to "things one can do at a large scale that cannot be done at a smaller scale." Mayer-Schönberger and Cukier (n 30) 6. While there should be a healthy skepticism, or as Hildebrandt puts it "constructive distrust" in the "objectivity, reliability and relevance" of big data derived insights, the belief in the possibility of big data has been a powerful incentive for collection of data at scale. Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar Publishing Ltd 2015) 36.

[32] Mejias and Couldry (n 30) 2.

[33] Van Dijck (n 30).

[34] *See* Claude Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective' in Serge Gutwirth and others (eds), *European Data Protection: In Good health?* (Springer Netherlands 2012); Janice C Sipior, Burke T Ward and Ruben A Mendoza, 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons' (2011) 10 Journal of Internet Commerce 1.

[35] For example, Google's use of purchased credit card data. Mark Bergen and Jennifer Surane, 'Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales' *Bloomberg* (30 August 2018) <https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales> accessed 6 March 2019. Data brokers can be an important source of these types of data. See Matthew Crain, 'The Limits of Transparency: Data Brokers and Commodification' (2018) 20 New Media & Society 88; Giridhari Venkatadri and others, 'Auditing Offline Data Brokers via Facebook's Advertising Platform', *The World Wide Web Conference* (ACM 2019) <https://dl.acm.org/doi/10.1145/3308558.3313666> accessed 12 March 2023.

[36] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75; Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books Ltd 2019); Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27).

[37] Zuboff (n 36).

profiling purposes.[38] Cohen also considers this phenomenon, characterising it as extractive, as individuals become a resource to be exploited, in a transformation of the traditional business/user/customer relationship—one which Cohen conceives of as controlling in a dystopian, deterministic sense.[39]

Cohen's informational capitalism looks more broadly to a new phase of political economy, that is "the alignment of capitalism as a mode of production with informationalism as a mode of development."[40] While Zuboff's descriptive model of the emergence of surveillance capitalism is very valuable, it has limitations in isolating particular business models from capitalism more broadly and in the overly simplistic vision of the law's relationship to surveillance capitalism.[41] Cohen, on the other hand, puts law at the centre of her exploration of data's political economy.[42] Legal institutions cannot be separated from the political economy which they have shaped, and in turn by which they have been shaped, and both can be contextualised within prevailing ideologies.[43] In this way, datafication and informational capitalism are intrinsically linked. Moreover, Cohen is concerned with how legal regulatory and institutional structures have enabled the accumulation of power, and this has been influential in my construction of this thesis. In particular, in investigating the role and conception of the individual in an environment of mass datafication and informational capitalism, I am not only interested how data protection law reacts, but also how data protection law enables.

3. The contribution and literatures

This PhD is situated in and contributes to the literature on information privacy and data protection. My thesis's contribution may be summarised in two parts. First, my thesis offers a more detailed account of the legal role of the individual in EU data protection law than previously made, an analytical framework against which this role may be understood and assessed, and an evaluation of this multi-faceted role of the individual. Second, my thesis connects this debate regarding the place of the individual in privacy and data protection law with the question of legal personhood, or theories of the person in law. I demonstrate that the legal role of the individual in EU data protection law is connected to the idea of the person, and assumptions regarding their nature and function in relation to law. In this section, I summarise the main relevant literatures which are engaged in this question,[44] in order to contextualise where my contribution sits.

The question of the individual has emerged in privacy and data protection literature in a number of ways. First, a number of scholars have criticised the law as individualistic, which is characterised as inadequate to deal with contemporary data processing practices. This criticism is often founded in examinations of rights-based approaches to privacy. In the US context, a number of scholars have argued for a re-conceptualisation of privacy away from the individual. Thus, Regan and Solove have both argued that individualised rights to privacy

---

[38] ibid.
[39] Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27).
[40] ibid 5.
[41] For example, see Zuboff's discussion of the GDPR. Zuboff (n 36) 480–488. This is a criticism which Cohen has also made of Zuboff's work. Julie E Cohen, 'Review of Zuboff's The Age of Surveillance Capitalism' (2019) 17 Surveillance & Society 240. See also Amy Kapczynski, 'The Law of Informational Capitalism' [2020] The Yale Law Journal 1460.
[42] Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27).
[43] ibid.
[44] As noted in Section 1.3 above, only English language literature has been considered, and therefore the contribution should be understood in this regard.

tend to be undervalued or outweighed by countervailing interests,[45] and Schwartz has argued for a democratic foundation for privacy.[46] Many have contrasted individual rights-based approaches with social perspectives. Nissenbaum looks to privacy as a social issue, locating individuals within their social contexts to develop a framework of "contextual privacy".[47] Viljoen has argued that individualist conceptions of privacy harms fail to account for the social effects of the data economy.[48] Waldman criticises individual rights-based approaches to privacy as ignoring the social nature of privacy, and further argues that self-management approaches practically undermine privacy due to their abuse by industry practices.[49]

In the context of her book on the relationship between law and informational capitalism, Cohen has critiqued the centrality of the individual from a critical theory lens, locating the primacy of the individual in informational privacy in its liberal political philosophy and subsequent neoliberalism.[50] She extends this critique to the conventional legal institutional approach to information privacy, arguing that "the traditional emphasis on individualised claims and individuated process resonates with neoliberalism's emphasis on marketized, and individualised choice."[51] Cohen's work is primarily focussed on the US legal system, but she does note the European approach to the regulation of the information economy as a point of contrast, acting "more aggressively"[52] and at the same time worries that "important strands of discourse about individual autonomy present opportunities for co-optation by corporate claimants", and notes "potentially fatal implementation difficulties."[53] She argues that the success or failure of European data protection is contingent on a number of factors, including: regulatory enforcement and the development of accountability mechanisms "that do not rely exclusively on individualised autonomy and control claims to secure their realization".[54] This aligns with her broader conclusion that "[a]rticulations of fundamental rights designed to defend and extend liberal individualism must be paired with others that engage directly with the logics of neoliberal governmentality and platform-based, data-driven, algorithmic power."[55]

Similarly, in Europe, there has been some criticism of the effectiveness of individual rights approaches. Often these criticisms are rooted in societal or group harms associated with contemporary data processing practices (such as AI or big data) and argue an individual rights approach is lacking in light of such challenges. Thus, de Hert and Papakonstantinou advocate for looking beyond individual rights, characterising such a perspective as "unfit for

---

[45] Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press 1995); Priscilla M Regan, 'Privacy as a Common Good in the Digital World' (2002) 5 Information, Communication & Society 382. Daniel J Solove, 'The Meaning and Value of Privacy', *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 74. Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1881.

[46] Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review; Nashville 1609.

[47] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010).

[48] Salome Viljoen, 'Democratic Data: A Relational Theory For Data Governance' (2021) 131 Yale Law Journal 573.

[49] Waldman, Ari Ezra;, 'Privacy, Practice, and Performance' (2022) 110 California Law Review 1221.

[50] Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27) 7.

[51] ibid 145.

[52] ibid 177.

[53] ibid 262.

[54] ibid 263.

[55] ibid 271.

the collective problems and challenges of Big Data and Big Data analytics."[56] Similarly, Smuha has questioned how societal harms associated with AI can be addressed when the legal system is primarily concerned with individual rights and remedies.[57] In the context of genetic data, Costello, and Kuru and Beriain have separately questioned the fit with individualised approaches.[58] Blume was also notable in questioning and examining the category and conception of the data subject within data protection law.[59]

Three scholars in particular have offered more comprehensive consideration of the nature and consequences of individualist perspectives in EU data protection or privacy law: van der Sloot, Bieker and Lindroos-Hovinheimo. Van der Sloot is notable for considering the place of the individual in a 2014 article and his 2017 monograph.[60] In his 2014 article, he takes a historical viewpoint on the role of the individual, noting that the subjective individual approach to data protection has achieved greater prominence over time,[61] a shift which has been seen more broadly in policy development,[62] and he then argues that an individualised approach based on informational self-determination should be re-problematised in light of current data processing practices, particularly the societal impact of the rise of Big Data.[63] This problematisation is taken further in his 2017 monograph, in which he argues that the conventional paradigm of balancing an individual right to privacy against competing interests "no longer holds in an age of Big Data".[64] While his 2014 article considered the EU legislative approach to data protection, his 2017 monograph is rooted in fundamental rights-based approaches. Individual privacy rights, he argues, are less effective where individual harm identification is challenged, and accordingly individuals may not be well placed to seek to defend their rights and courts may not be well placed to assess the individual interest to be weighed.[65] The right to data protection, characterised as based on individual rights to control and invoke subjective rights is similarly challenged where individual identification by data processing is not necessary or prevalent.[66] This van der Sloot frames as a mismatch between the level of the data processing violation and the level at which remedies are provided—"The potential violation takes place at a general and group level and while it can be connected to individual concerns, this is increasingly besides the point."[67] Therefore, he advocates for a move to a conception of privacy and data protection founded on virtue

---

[56] Paul de Hert and Vagelis Papakonstantinou, 'Framing Big Data in the Council of Europe and the EU Data Protection Law Systems: Adding "Should" to "Must" via Soft Law to Address More than Only Individual Harms' (2021) 40 Computer Law & Security Review 105496, 8.

[57] Nathalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review <https://policyreview.info/articles/analysis/beyond-individual-governing-ais-societal-harm> accessed 7 December 2021.

[58] Róisín Á Costello, 'Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?' (2022) 22 Human Rights Law Review ngab031; Taner Kuru and Iñigo de Miguel Beriain, 'Your Genetic Data Is My Genetic Data: Unveiling Another Enforcement Issue of the GDPR' (2022) 47 Computer Law & Security Review 105752.

[59] Peter Blume, 'The Data Subject' (2015) 1 European Data Protection Law Review 258.

[60] B van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307; Bart van der Sloot, *Privacy as Virtue: Moving beyond the Individual in the Age of Big Data* (Intersentia 2017).

[61] van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60) 309.

[62] ibid 320.

[63] ibid 322–325.

[64] van der Sloot, *Privacy as Virtue* (n 60) 2.

[65] ibid 3.

[66] ibid 4.

[67] ibid 6.

ethics, which is concerned with the obligations of the data using agent.[68] Ultimately, he concludes that individual rights-based approaches "will need to be preserved to address issues in which individual interests are at stake",[69] but also integrating broader sets of requirements which bind data using agents, grounded in virtue ethics, in order to develop a vision for broader structural concerns.

Bieker's work on structural data protection also relates to the question of the individualism of the EU data protection regime. His book is grounded in the idea that data processing practices have societal and democratic impact.[70] His analysis of data protection law separates what he calls "individual data protection law" and "structural data protection law".[71] Arguing that almost all current discursive approaches to the right to data protection are anchored in notions of privacy, he contends that such approaches address "the issue posed by data processing only in terms of intrusions against an individual," and are thus incomplete.[72] He then makes a normative case for a re-conceptualisation of the right to data protection. His model, which he names the "dualistic approach" to data protection is said to differentiate individual and structural data protection, the latter referring to "the systemic aspects of data protection, such as institutional guarantees and organisational requirements."[73] This approach is based on fundamental principles which he derives from the legislative regime, which he characterises as "truly reflective of [the] material content" of EU data protection law.[74] He contends that individual and structural dimensions "are inherent in all the fundamental principles" of EU data protection law.[75] He then draws on these fundamental principles so derived to offer a reinterpretation of the fundamental right to data protection, in alignment with broader principles of democracy and the rule of law,[76] and an interpretation which touches upon the individual and structural dimensions of data protection law.[77]

Lindroos-Hovinheimo looks to EU privacy law from an alternative perspective, primarily interested in subjectivity, and asking "what kind of person is constructed in contemporary privacy law?"[78] Lindroos-Hovinheimo takes EU privacy law (so-described) as a site for the investigation of legal theories of personhood, grounded in continental philosophy, and in doing so is interested in the philosophical foundations of EU privacy law.[79] In deconstructing the person in European privacy law, she argues that the primary understanding of the subject is one of a "person in control", and links this to liberal individualism.[80] She argues that privacy rights operate to individualise persons from their community, and purely

---

[68] ibid 6–7.
[69] ibid 187.
[70] Felix Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*, vol 34 (TMC Asser Press 2022) 2.
[71] ibid 5.
[72] ibid 8.
[73] ibid 182.
[74] ibid 205. These principles bear resemblance to the 'core principles of data protection' identified and described in Bygrave's earlier work. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 18) ch 3.
[75] Bieker (n 70) 206.
[76] ibid 226.
[77] ibid 229.
[78] Susanna Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (Cambridge University Press 2021) 171.
[79] Katherine Nolan, 'Book Review: Private Selves: Legal Personhood in European Privacy Protection' (2021) 7 European Data Protection Law Review 624.
[80] Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78) ch 3.

subjective approaches to privacy should be rejected as a result.[81] Lindroos-Hovinheimo calls for an alternative to the liberal "possessive individualism" she contends has shaped European privacy rights, based on a pluralistic conception of the subject, beginning from an idea of community.[82]

Alongside these works, we see particular questions about the individual and their role occur across many strands of EU privacy and data protection law scholarship. Van Alsenoy, Edwards et al, Chen et al and Finck have all examined the issue of the individual being classified as a data controller.[83] Ausloos and Mahieu have separately considered the legal role of the individual within the context of particular data subject rights.[84] A number of scholars have reflected on the place of the individual in the context of debates over informational self-determination. For example, Bygrave and Schartum have reflected upon the link between the individual and the philosophy of data protection, observing that "the ideological basis for data protection law and policy, […] accords a central place to the autonomy and integrity of the individual *qua* individual."[85] Such considerations are also found in the works of Purtova, Lynskey and Bietti.[86] Questions on the role of the individual have also arisen in the context of consideration of the scope of data protection[87] and enforcement issues associated with data protection.[88]

It is unsurprising that the individual and questions of their status and conception within the EU data protection regime are the subject of this variety of existing works, as this reinforces the claim that I advance herein – that the individual, their legal role and conception are central to the regime. My contribution builds upon and has some commonalities with these existing works, but also important differences and additional contributions.

---

[81] ibid ch 4.
[82] ibid ch 6–7.
[83] Brendan Van Alsenoy, 'The Evolving Role of the Individual under EU Data Protection Law' [2015] CiTiP Working Paper Series 36; Lilian Edwards and others, 'Data Subjects as Data Controllers: A Fashion(Able) Concept?' (*Internet Policy Review*) <https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400> accessed 21 October 2019; Jiahong Chen and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279; Michèle Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 International Data Privacy Law 333.
[84] Jeff Ausloos, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection* (Oxford University Press 2020); Rene Mahieu, 'The Right of Access to Personal Data: A Genealogy' [2021] Technology and Regulation 62.
[85] Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 169.
[86] Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table … and Back on Again?' (2014) 30 Computer Law & Security Review 6; Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40; Nadezhda Purtova, 'From Knowing by Name to Targeting: The Meaning of Identification under the GDPR' [2022] International Data Privacy Law ipac013; Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015); Elettra Bietti, 'The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond' [2020] Hoover Institution Aegis Paper Series 16; Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 European Journal of Law and Technology 26.
[87] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86); Dalla Corte (n 86).
[88] Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 International and Comparative Law Quarterly 799.

First, my thesis might be said to share the interest of others in the place of the individual, and a certain scepticism of individualist approaches, or at least the implementation of certain aspects relating to the individual. Further, along with Cohen, Van der Sloot and Lindroos-Hovinheimo in particular, my thesis shares an interest in the philosophical underpinnings of EU data protection law, and how these connect to the role and conception of the individual within the legal regime.

Further, in extending these literatures, my thesis may be said to make an additional and original contribution.

First, my analysis, rooted in the legislative scheme of the GDPR alongside the case law on the right to data protection offers a more detailed account and deeper understanding of the role of the individual in EU data protection law.[89] Few have looked directly to the legislative scheme of EU data protection, rooted in a rights-based approach, but which is characterised by its legislative features. Other accounts to date have not had such a focus—rather, they were primarily concerned with privacy or data protection rights, such as van de Sloot,[90] or grounded in CJEU cases and the issues raised therein rather than the full scope of the legislation, such as Lindroos-Hovinheimo.[91] While Bieker considers the legislative regime, he does not engage deeply with that which he calls 'individual data protection law', but rather briefly defines these aspects of the law as those which "aim to safeguard the interests of data subjects and/or award them specific enforceable rights."[92] Each of these scholars foreground issues of the individual in order to move to and suggest or construct alternative normative visions of data protection, while my thesis suggests that the foregrounding requires more attention, particularly in the EU where the right to data protection finds its expression in the legislative scheme, and is rooted in particular historical and institutional contexts. Thus my thesis seeks to integrate considerations of the right to data protection, the GDPR and associated case law in our understanding of the individual and their place within the EU data protection regime, and offers new doctrinal, contextual and conceptual understandings of the role and conception of the individual across the regime.

Second, in discussing the conception, or notion of the individual, as expressed in EU data protection law, I am offering a further dimension to the problematisation of the regime, and in particular those aspects of the regime which are connected to the individual. The question of *who is the individual* who underlies the data subject or natural person in the regime has received little attention, with the exception of Blume and Lindroos-Hovinheimo.[93] By questioning the understanding of the individual—their capacities, situation and relation with

---

[89] For example, some scholars have characterised the regime as one of notice and control, in their account of the individualist nature of the regime, whereas I contend that the picture is broader than that. For example, Costello characterises the EU architecture as "premised on notice and control", in order to point to individualism in European privacy law. Costello (n 58) 4–8.

[90] van der Sloot, *Privacy as Virtue* (n 60). By design, as van der Sloot explicitly acknowledges. ibid 7–8. A rights-based approach to privacy is also the focus of many of the US scholars who write on information privacy rights, see fn 45 - 49 above.

[91] Lindroos-Hovinheimo's work is valuable, but not comprehensive on the topic, she herself acknowledges that her case method does not result in an exhaustive consideration of EU data protection law. Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78) 168.

[92] Bieker (n 70) 186.

[93] Peter Blume was first to note that there is little acknowledgment of the different experiences and capabilities of different types of person in this regulatory regime. Blume (n 59). Lindroos-Hovinheimo's valuable study (discussed above) aims to uncover the theory of personhood which underlies EU data protection law. Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78).

others—new revelations about the assumptions and philosophies (at times fragmentary or contradictory) of EU data protection law emerge. This is achieved by bringing EU data protection law in conversation with literature on theories of legal personhood; personhood within the EU framework,[94] the notion of relational personhood,[95] ideas of empowerment and paternalism,[96] and ideas of homogeneity and difference.[97] In linking these literatures with new doctrinal analyses of the EU data protection regime, this thesis contributes a new understanding of the notion of the individual which underlies the regime, and how key issues at the heart of the debate on the effectiveness of data protection are rooted in questions regarding the individual.

Additionally, there is a complementary set of literature to which my thesis might be said to operate in parallel. While my thesis does not seek explicitly to further the idea of "collective data protection", or "group privacy", this is a topic which has attracted increasing attention. In association with critiques of individual privacy or data protection, a number of commentators have located the natural alternative in group or collective approaches.[98] For example, Taylor et al have argued that in the age of big data, protection of the individual should be supplemented, by looking to information which identifies categories or groups.[99] The commercial value in such big data technological developments is often associated with clustering of groups, rather than on identifying individuals.[100] Therefore, they argue, "[a]s algorithmic societies develop, attention to group privacy will have to increase."[101] Similarly, Floridi advocates for the protection of the privacy of groups, as to do otherwise is to underestimate the risks associated with profiling and analytics run over large data sets.[102] When the focus of information technologies is often to classify people in groups rather than as individuals, Floridi argues, "[s]ometimes the only way to protect a person is to protect the group to which that person belongs."[103] Further, a number of scholars have used the economic language of a public or common good to argue for a re-conceptualisation of privacy in such collective terms.[104]

---

[94] See Chapter 3.
[95] See Chapter 4.
[96] See Chapter 5.
[97] See Chapter 6.
[98] Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 Ethics and Information Technology 275; Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 Computer Law & Security Review 238; Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-46608-8> accessed 2 December 2020; Ugo Pagallo, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017); Luciano Floridi, 'Group Privacy: A Defence and an Interpretation' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017).
[99] Linnet Taylor, Luciano Floridi and Bart van der Sloot, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017) 5.
[100] ibid 10.
[101] ibid.
[102] Floridi, 'Group Privacy: A Defence and an Interpretation' (n 98) 98.
[103] ibid 97–98.
[104] Including, Regan (n 45); Joshua Fairfield and Christoph Engel, 'Privacy as a Public Good' (2015) 65 Duke Law Journal 385; Dennis D Hirsch, 'Privacy. Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel' (2016) 65 Duke Law Journal 67; Henrik Skaug Sætra, 'Privacy as an Aggregate Public Good' (2020) 63 Technology in Society 101422.

In the EU data protection context, Mantelero explores the concept of "collective data protection".[105] Again, considering forms of analytical classification which try to predict group behaviour,[106] Mantelero is concerned that such classification may enable unfair discrimination against various groups.[107] Rather than looking to individual harm, Mantelero classifies the interests in such data processing as non-aggregative, and as such better represented by the fundamental values of a given society.[108] Pagallo is sceptical of the recognition of group rights (as corporate entities) in EU data protection law.[109] He argues to introduce corporate group rights could undermine autonomy and anti-paternalism, which is not in the spirit of EU data protection law.[110] As to the protection of group rights as collective rights, Pagallo says such new regulation should only be introduced on the basis of empirical evidence of relevant harm and the capacity of collective rights to redress such harm.[111]

My thesis also contributes to this debate, which frames the debate over individualism on a individual-collective spectrum, in two ways. First, by offering a framework specifying the particular aspects of the EU data protection regime which are centred around the individual, and those which are less individually-oriented, and contrasting those which are less so, it offers a more targeted and accurate understanding of the law to contrast with proposed collective approaches. Second, by offering an account of the individual's role in EU data protection law which is rooted in the underlying ideas and assumptions implemented in the law, it may also serve to problematise the assumption that collective approaches to data protection will necessarily overcome the challenges associated with individualist approaches.

Finally, the related question as to the extension of data protection rights to legal persons or collective entities is also relevant. Bygrave has engaged in an extensive study as to the question of the extension of data protection rights to collective entities.[112] Bygrave notes that data protection rights are conferred upon collective entities in a number of EEA countries.[113] The extension of such rights to collective entities, he argues, is not excluded by either the common usage of the concept of privacy nor by functions and values of privacy.[114] Bygrave's study is notable for highlighting the link between technological change, particularly "electronic interpenetration" of new spheres of activity, and how that calls into question the shift from the individual to collective or systemic considerations.[115] Mantelero characterises this type of protection as one of "organisational privacy", and notes it concerns both the legal person's claim to privacy, but also indirect protection of the underlying individuals who constitute that collective.[116] Walden and Savage, in their early work on this question, considering potential extension of privacy and data protection laws to organisations, also connect the question to the group privacy of the underlying natural persons.[117] This question, regarding the extension of privacy or data protection rights to legal persons or collective

---

[105] Mantelero (n 98).
[106] ibid 246.
[107] ibid 247.
[108] ibid 249.
[109] Pagallo (n 98).
[110] ibid 163.
[111] ibid 171.
[112] See Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 18), Part III.
[113] ibid 186.
[114] ibid 242.
[115] Ibid 13.
[116] Mantelero (n 98) 242.
[117] IN Walden and RN Savage, 'Data Protection and Privacy Laws: Should Organisations Be Protected?' (1988) 37 International and Comparative Law Quarterly 337.

entities, thus has two important points of interconnection with my thesis. First, it could be regarded as a subset of the literature on group/collective data protection, mentioned above, and the same contribution is made in terms of offering a framework for understanding the role of the individual and a problematisation of advocating for collectivist solutions without having regard to underlying ideas and assumptions of personhood. Second, the extension of data protection rights to different types of legal persons (corporations, collective entities or other legal persons) also has implications for the relationship between such rights and individual natural/physical persons. The notion that such rights could be applied to legal persons in the same manner as to natural persons has interesting implications for the conception of personhood which underpins EU data protection law. This issue is beyond the scope of this thesis, but is reserved for future work.

4. Summary

In Chapter 2, *The multi-faceted role of the individual,* I present a framework for understanding the ways in which the individual is central to the framing and operation of data protection law. This centrality is seen through the examination of the multi-faceted role which the individual is playing, each facet central to various aspects of data protection law; its objectives, its scope, its interpretation, its determination of legality and its enforcement. In each of these areas of the law, the individual's interest and actions are prominent, though not entirely determinative in an absolutist individualist sense.

Individual protection serves as the normative foundation for the operation of EU data protection law, a source of its legitimacy as well as the driving force in its interpretation and operation. The individual shapes the subject matter of regulation, as their interests shape the scope of EU data protection law and are central to the assessment of legality under the GDPR. The individual is also critical to the operation of data protection, as they challenge data controllers and protect their own interests, and their decision making over data is granted legal status.

Each facet of the individual's role is then questioned. The identification of the individual as the normative foundation of data protection may be underinclusive of group or societal concerns, particularly in light of the individualist interpretation that the CJEU takes of the right to data protection. The protection of an individual as an individual subject is not inevitable, and indeed, alternative approaches do seem compatible with the regime when we consider the rules governing sensitive personal data. The designation of an individual as a regulated controller seems unlikely to be practically desirable in some cases given the bureaucratic nature of many controller obligations. The role of the individual as an agent of data protection law, as decision-maker and enforcer, comes under strain in light of the scale of datafication individuals face and therefore questions of improper responsibilisation arise.

In Chapter 3, *Shifting ideas of the individual,* I examine some of the factors which explain why the individual has come to be central to the EU data protection project. This contribution argues that we should understand the centrality of the individual as connected, in part, with two important contextual developments. The first is the historical and conceptual connection of data protection to rights to privacy/respect for private life, and the emergence of European rights frameworks in the enlightenment era. The second is the European Union context itself, particularly the shaping forces of the EU's economic order and its growing fundamental rights mission. The place of the individual within each of these projects, and the tension between the two which sometimes occurs are introduced. Once recognised, these contextual factors allow us to look to the nature of the individual which has taken shape in

EU data protection law. The individual who manifests in the current legal regime is unsurprisingly not an entirely coherent or unitary construction, but rather conflicting ideas of personhood are evident. One such conflict is explored, as I argue that the individual is seen as both a citizen rights-holder within the regime, and also as a consumer and economic object. This exercise reinforces the relevance of the idea or conception of the individual in EU data protection law as a fruitful means by which to engage with the law. Ideas which underpin the law, about the nature of the individual, and their relationship with the law and the market, once resurfaced can be examined anew.

In Chapter 4, *The relational individual and plural personal data*, we continue our exploration of the conception of the individual in EU data protection law, according to the parameter of relationality versus individuation. By introducing the concept of "plural personal data" as a proxy for different types of relationality, we can engage with the extent to which existing EU data protection law can accommodate relational understandings of the person. What emerges is a partial recognition of plural personal data by the CJEU, and fragmentary recognition of it in the GDPR, but a dominant understanding of the individual as individuated from others. In examining how the law applies to plural personal data, a number of challenges are highlighted, particularly deriving from those aspects of the law which tend towards individualism. Plural personal data can challenge the threshold for application of the law, assessment of the legality of processing and the exercise of individual data subject rights. This raises questions as to the desired reach of the GDPR, and the extent to which it aims to act beyond individual impact, and the issues created when multiple persons may be affected by the same processing activity within the same data. The challenges of the application of EU data protection law to plural personal data highlights an individuated conception of the data subject, often ignoring subjects' relationships with others which contribute to interdependent and interconnected nature of data processing.

In Chapter 5, *The empowered individual versus data protection paternalism,* I offer an account of the ways in which EU data protection law seeks to both empower and paternalistically protect the individual. This account operates at three levels: substantively (with regard to the purposes to which data may be used), procedurally (to defend an individual's legal interests and rights) and structurally (to create an environment within which the individual may be protected or empowered.) This framework allows us to both articulate and assess this key balance in EU data protection law. What emerges is a greater prevalence of paternalistic strategies than is commonly presented, though without a cohesive conceptualisation of what the paternalistic protective strategy of EU data protection law is. The conception of the empowered individual emerges as a marketized subject, as the GDPR borrows from marketplace concepts and strategies in its legislative approach.

In Chapter 6, *Difference, uniformity and the individual,* I examine the balance between uniform and differentiated approaches to the individual as data subject. Through an examination of how the subject is treated, I argue that EU data protection law can accommodate some degrees of difference between data subjects. This differentiation is seen first in the application of individualised standards, as the Court has begun to consider how specific and individualised legal compliance by controllers must be. Second, there is express recognition of some types of difference, through the protection of special categories of data, and particular categories of data subjects (children and vulnerable data subjects). A patchwork understanding of difference emerges, perhaps associated with historical patterns of discrimination. However, not all types of difference may be recognised or accommodated, and moreover, exclusionary assumptions about personhood are embedded in the law.

In the Conclusion, I reiterate the key findings of this thesis, and offer some reflections on the significance of my contribution and questions for further research. Questions as to the conceptual foundations of data protection persist. We come to see that key dilemmas of EU data protection law are connected to the place and understanding of the individual in the law: issues of scale and structural forces affecting data protection, the enforcement of data protection law, and the capacity of law to redress a broad range of harms in a diverse pluralistic Europe.

CHAPTER 2: THE MULTI-FACETED ROLE OF THE INDIVIDUAL

1. Introduction

The first step to assessing or evaluating the role of the individual in data protection law is to understand it. It is surprising, therefore that in light of growing criticism of "individualism" in data protection and privacy law, there has been no detailed elucidation of the role of the individual,[118] against which we can evaluate the claims that an individually oriented data protection law is failing. This chapter offers such a contribution. While this framework cannot be said to be exhaustive,[119] the model presented is more comprehensive than found in scholarship to date, and thus provides a valuable basis upon which to begin to assess such claims about the nature of the individual in EU data protection law.

While the data protection regime cannot be said to be entirely individualistic, I argue that the individual is central to the regime. The role of the individual is multi-dimensional, and the individual serves as the normative foundation, the central legal subject and an agent of EU data protection law.

1.1. The role of the individual: normative foundation, legal subject and agent

The individual plays a central but multi-faceted role in EU data protection law. Through an examination of the framework of the GDPR, its predecessor, the Data Protection Directive, Article 8 of the Charter, Article 8 ECHR, the associated case law of the CJEU and selected leading case law of the ECtHR, it can be said that the individual serves as the normative foundation, the central legal subject and an agent of EU data protection law.

Rather than taking a normative position, this conceptual model is built upon a doctrinal analysis of the current, multi-partite role the individual is playing within the regime. The conceptual model was developed through an inductive reading of the relevant legislation (the Data Protection Directive and GDPR) and case law relating to those legal instruments and Article 8 of the Charter and Article 8 ECHR. The method of review was doctrinal, informed by the qualitative method of thematic analysis,[120] in order to be systematic in the review of the materials and to be cognisant of the process of assigning analytical labels to themes in the case law and legislation.[121] The legislation and decisions were coded, identifying aspects of the legislation or decisions which related to the individual. Once coded, the codes were then grouped into thematic classifications, in order to allow analysis according to those themes.

---

[118] Lindroos-Hovinheimo contributes a wonderful work on the philosophy of the person underpinning EU data protection law, but does not engage in a doctrinal categorisation such as is offered herein. Lindroos-Hovinheimo (n 78).

[119] See Introduction, section 1.3.

[120] On the process of thematic analysis, see Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2006) 3 Qualitative Research in Psychology 77; Jennifer Fereday and Eimear Muir-Cochrane, 'Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development' (2006) 5 International Journal of Qualitative Methods 80.

[121] For similar adoption of an inductive qualitative approach for the review of case law, see for example: Saïla Ouald Chaib, 'Procedural Fairness as a Vehicle for Inclusion in the Freedom of Religion Jurisprudence of the Strasbourg Court' (2016) 16 Human Rights Law Review 483.

This was an iterative process, in which cases and thematic classifications were revisited in light of parallel reading in academic literature and overall themes were identified.

The thematic categorisation which emerges is that of the individual as the normative foundation, the central legal subject and an agent of EU data protection law.[122] The individual is the normative foundation of EU data protection law in the sense that the courts and legislature take the individual and their interest as their object in the design, implementation and enforcement of EU data protection law. More specifically, the protection of the individual and their fundamental rights provide the normative basis and primary law competence justifying the regime, and this explicit role has driven a purposive approach to the interpretation of data protection law.

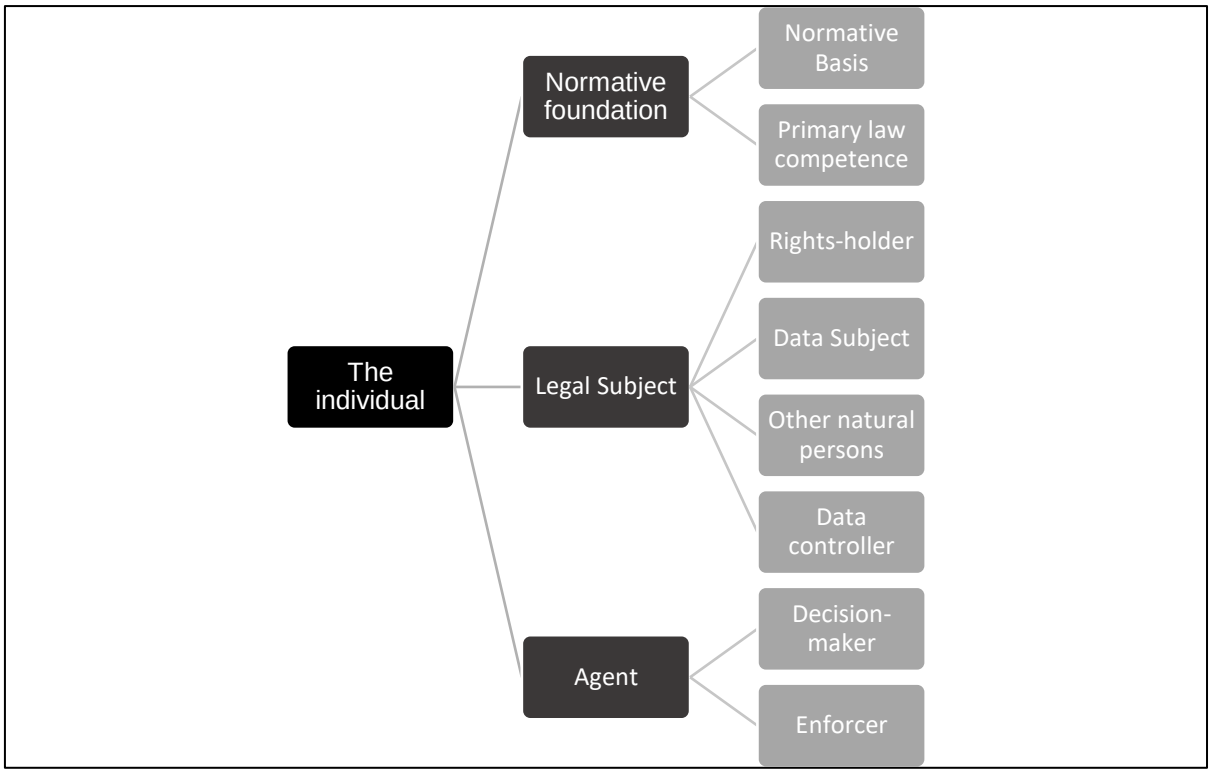
The individual is also an important legal subject of data protection law, which can arise in a variety of ways. As a rights-holder, the right to data protection attaches to the individual, and they can wield this right to important effect. As a protected actor under data protection legislation (the "data subject"), the individual comes to be central to the logic of the regime, particularly to the scope of the law, as well as the assessment of legality under the GDPR. Moreover, the individual may also be a regulated subject of data protection law as a data controller, the responsible entity in data protection law.

Finally, the individual is also a participant in the operation and enforcement of data protection law, which I name "an agent" of data protection law.[123] Through the protection of individual decision making and the grant of procedural rights to the individual, the individual is one of the actors in the regime through which the protection of personal data is completed.

This multi-faceted role of the individual is depicted below.

[122] A number of scholars have either pointed to or advocated for this central role of the individual as the normative foundation of EU data protection law. See Bygrave and Schartum (n 85); Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86); Lynskey, *The Foundations of EU Data Protection Law* (n 86).

[123] This designation is inspired by the observations of EU scholars on the role of the individual as an agent in the completion of the EU project. JHH Weiler, 'Van Gend En Loos: The Individual as Subject and Object and the Dilemma of European Legitimacy' (2014) 12 International Journal of Constitutional Law 94; Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places, 'Being a Person in the European Union' in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016).



Once thus conceived, this conceptual model offers a framework for more nuanced normative evaluation of EU data protection law, and the place therein. We build a more detailed picture of the extent of the law's "individualism", and can tease out and differentiate the components thereof – whether the individual should serve as the normative foundation, or a central legal subject, or as an agent of EU data protection law?

2. The individual as the normative foundation of data protection law

As the object of the adopters and enforcers of EU data protection law, the individual and the protection of their rights and interests serve as the normative foundation for the regime. This normative status has legal significance in three important ways to be explored: first, the primary law competence to adopt EU data protection legislation under the Treaties is linked to the individual, second, the purposive interpretation adopted by the CJEU is driven by the individual interest.

2.1. The normative basis for EU data protection legislation

This normative basis for EU data protection legislation has undergone some transition over time, but from the outset has been linked to the protection of the individual.

The Data Protection Directive had two express aims: the free flow of personal data throughout the EU and the protection of the rights and freedoms of individuals.[124] The right to privacy was conceived as the particular basis for protection of individuals.[125] Alongside this desire to protect individual interests, the Data Protection Directive was also adopted as a

[124] Article 1, Data Protection Directive.
[125] See Recital 2, Data Protection Directive: *Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*. (My emphasis). See also Recitals 7, 9-11, 33-34, 68, Article 1(1), Data Protection Directive.

measure of market harmonisation. In order to facilitate the completion of the single market, and associated cross-border flows of data, harmonisation of privacy standards was seen to be necessary.[126] Thus, at its outset, EU data protection law had two primary goals, with the need to reconcile the protection of the individual with the market harmonisation aim.[127]

Over time, the basis for data protection in the EU changed. While the Data Protection Directive made reference to the protection of privacy, in particular as recognised by Article 8 of the ECHR,[128] the introduction of new rights protections and a specific legal competence was significant. The Lisbon Treaty introduced new legal status to data protection, with an explicit competence for data protection and recognition of the right to data protection.[129] Additionally, and importantly, the EU Charter of Fundamental Rights was adopted and became part of the EU constitutional order, with equal status to the Treaties. The Charter contains an explicit standalone right to the protection of personal data,[130] alongside the right to respect for private life.[131] The Charter has played an increasingly prominent role in the CJEU's decision making,[132] as predicted by Lynskey, who notes that EU data protection has transitioned from a measure of market harmonisation with high protection of fundamental rights and freedoms to a regime with a fundamental rights orientation.[133]

The GDPR, adopted in 2016 and replacing the Data Protection Directive, still acknowledges the desire to achieve free movement of personal data throughout the EU,[134] but is more firmly grounded as a fundamental rights instrument. The substance of the rules of the GDPR is to protect individuals, grounded in the right to data protection.[135]

In its focus on the protection of data protection as a fundamental right, the normative legitimacy of the GDPR is grounded in the protection of the individual. The fundamental right to data protection may have emerged after data protection legislation,[136] but it has consolidated existing emphasis on the individual in predecessor legislation. In this shifting emphasis, the GDPR reflects the emergence of the EU fundamental rights project.[137] The GDPR imposes compliance obligations upon controllers, which necessarily interferes with the freedoms and interests of others, including the freedom to conduct a business,[138] and

---

[126] Recitals 5, 8, Data Protection Directive.
[127] Of course, these objectives are not framed in absolutist terms and in the implementation of these objectives through legislation, other rights and interests come to be balanced with such objectives, but as we shall see, the express objectives have important legal significance. See section 2.2. below.
[128] Recital 10, Data Protection Directive.
[129] Article 16, Treaty on the Functioning of the European Union.
[130] Article 8, Charter.
[131] Article 7, Charter.
[132] See discussion in section 2.2(b) below.
[133] Orla Lynskey, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Netherlands 2013).
[134] Article 1(1) of the GDPR provides: "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data." Article 1(3) provides that "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."
[135] See discussion in section 3 below.
[136] See e.g. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014); Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (Oxford University Press 2019).
[137] See González Fuster (n 136) ch 5.
[138] Article 16, Charter.

the freedom to engage in work and provide services.[139] These interferences are said to be necessary or justified because of the need to safeguard affected individuals. Despite being a Regulation in name, there is substantial room for Member States to derogate, thus limiting its capacity to ensure free movement of data throughout the Union,[140] and explicitly sets out to assure the protection of the fundamental right to data protection. The free market objectives of the Regulation thus have been subsumed by the need to protect individuals. On its own terms, therefore, the success of the GDPR can be judged in accordance with its ability to effectively protect individuals.

2.2. The legal significance of the objective of individual protection

(a) Primary law basis for EU data protection law

Under the principle of conferral, the EU may only act where it has been conferred with an express competence under the Treaties.[141] After the Lisbon Treaty, along with the adoption of Article 8 of the Charter, there was a change in competence for the adoption of EU data protection law. The Data Protection Directive was adopted as a measure of market harmonisation.[142] As such, it was not tied expressly as a matter of competence to a rights-orientation or any substantive approach to data protection. However, over time, a shift in the primary law basis for EU data protection law has occurred, in line with broader constitutional and institutional shifts in the EU. Now, the legislature must act in order to protect the individual and their right to data protection.

After Lisbon, Article 16 of the Treaty on the Functioning of the European Union ("TFEU") was introduced as the basis for the adoption of EU data protection measures, founded on the right to protection of personal data, formulated as follows:

> *1. Everyone has the right to the protection of personal data concerning them.*
>
> *2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
>
> *The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.*

---

[139] Article 15, Charter.

[140] The GDPR allows Member States to introduce national variations on a wide number of GDPR provisions, including; the age of children's consent (Article 8(1), GDPR), additional conditions as to the processing of genetic data, biometric data or data concerning health (Article 9(4), GDPR), restrictions necessary to safeguard national security, defence, public security, criminal investigations and prosecutions and a series of other public interests (Article 23, GDPR), restrictions necessary to protect the right to freedom of expression and information (Article 85(1), GDPR), rules relating to public access to official documents (Article 86, GDPR), conditions for the processing of national identification numbers (Article 87, GDPR), conditions for the protection of employee data (Article 88, GDPR), derogations for scientific or historical research purposes or statistical purposes (Article 89, GDPR) or obligations of official secrecy (Article 90, GDPR).

[141] Article 5, Treaty on European Union.

[142] Grounded on the precursor to Article 114 Treaty on the Functioning of the European Union, which allows the EU to adopt measures for the approximation of laws in the interest of the establishment and functioning of the internal market.

In this way, the legislative basis for data protection initiatives is now explicitly linked to the protection of individuals and their fundamental right to data protection.[143]

Article 8 of the Charter provides further details for the nature of the right to data protection, in particular indicating some of the core aspects of the manner in which that right is to be safeguarded:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*

Article 8 of the Charter also should be interpreted in light of the associated right under the ECHR, Article 8 which respects the right to respect for private life.[144] Article 52(3) of the Charter provides that fundamental rights which have corresponding rights to those under the ECHR should be interpreted the same as those ECHR rights, though the EU can provide a higher level of protection.[145] The Court has accordingly expressly recognised that Articles 7 and 8 of the Charter must be interpreted in light of Article 8 of the ECHR, and that any limitations imposed on those rights must "correspond to those tolerated in relation to Article 8 of the [ECHR]."[146]

Thus, data protection now has its roots in EU primary law, and in its formulation, is expressly tied to a particular type of regime, founded on the protection of individuals with a rights-orientation.[147]

How the rights-orientation must inform the legislative implementation of Article 16(2) TFEU, such as the GDPR is still a matter of contention. For example, the question of whether a rights-based approach to data protection is necessarily absolutist or in opposition to a risk-

---

[143] As with Gellert, I prefer a non-absolutist vision of rights-based regulation. Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3.

[144] See further section 3.1 below.

[145] Article 52(3), of the Charter provides: "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection." See also Steve Peers and Sacha Prechal, 'Article 52 - Scope and Interpretation of Rights and Principles' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: a commentary* (2nd edn, Bloomsbury Publishing Plc 2021); Bruno de Witte, 'Article 53 - Level of Protection' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: a commentary* (2nd edn, Bloomsbury Publishing Plc 2021).

[146] C-92/09 *Volker und Markus Schecke and Eifert* [2010] I-11063, para 52.

[147] This transformation has been named the constitutionalisation of data protection law. Serge Gutwirth and Paul De Hert, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing data protection?* (Springer 2009). See also Federico Fabbrini, 'The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court' in Sybe A De Vries, Ulf Bernitz and Stephen Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years On*, vol 20 (Hart Publishing 2015) 266; Ausloos (n 84) 69.

based approach has emerged.[148] While this full debate is beyond the scope of this thesis, nevertheless we can see that the rights-based competence does seem to shape the permissible boundaries of data protection legislation. Hustinx questioned "how much flexibility Article 16 TFEU allows and where the impact of the Charter might pose certain limits."[149] As he notes, this is not simply theoretical.[150] During the development of the GDPR, the Council's Legal Service questioned the compatibility of the one-stop-shop mechanism with the right to an effective remedy.[151] More concretely, the CJEU has repeatedly confirmed that independent supervision is an essential component of data protection.[152] Similarly, the appropriate competence of the Canadian / EU PNR Agreement was the subject of judicial scrutiny, as the CJEU considered that an agreement to facilitate the sharing of passenger name data with Canada should have joint data protection and police cooperation.[153]

Thus, the individual as the normative basis for the data protection regime is cemented in EU primary law, the legislature must look to the individual's right in the adoption of data protection law, and this may serve to constrain reorientation or reimagination of the regime, should the criticisms of its individualistic tendencies be accepted.

(b) The purposive interpretation of data protection legislation

The objective of individual protection repeatedly appears in the case law of the CJEU through its use of purposive interpretation. Thus, as the legislature orients its activities to the individual and their rights and interests, the Court has adopted the individual interest in its interpretive approach. Many of the terms of the Data Protection Directive and GDPR are drafted at a high level of abstraction, and by interpreting these provisions in light of the aims of the legislation, the CJEU has had considerable influence on the shape of data protection law.

The desire to ensure free movement of data had some impact in the interpretation of the Data Protection Directive. It informed a judicial determination that data protection authorities ("DPAs") should ensure a fair balance between the right to private life and free movement of personal data in the exercise of their duties.[154] It also led to a finding that the Data Protection Directive amounted to generally complete harmonisation, and therefore precluded more onerous national implementation of its terms.[155] In *YS,* the CJEU emphasised that the concept of 'personal data' must be interpreted in light of the dual aims of the Data Protection Directive: the protection of fundamental rights and free movement of personal data.[156]

However, the need to protect individuals has received much more frequent and significant attention by the CJEU. Before the Charter was adopted, in *Rundfunk,* the Court found that

---

[148] See on this question Gellert (n 143); Raphaël Gellert, *The Risk-Based Approach to Data Protection* (1st edn, Oxford University Press 2020).
[149] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation' in Marise Cremona (ed), *New Technologies and EU Law* (Oxford University Press 2017) 166.
[150] ibid.
[151] ibid 161.
[152] ibid 166–167.
[153] Article 16 TFEU and Article 87(2)(a) TFEU; Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656), para 118.
[154] C-518/07 *Commission v Germany* [2010] ECR I-01885, par 24; C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650), para 42.
[155] Joined cases C-468/10 and C-469/10 *ASNEF* [2011] I-12181, para 29-39.
[156] Joined cases C-141/12 and C-372/12 *YS and Others* (ECLI:EU:C:2014:2081), para 41.

the Directive must "be interpreted in light of fundamental rights."[157] In particular, this was to be in light of Article 8, ECHR. In considering the national legislation at issue in that case, and its compatibility with the Data Protection Directive, the Court determined that the legislation first had to be assessed in terms of whether it interfered with private law, and if so whether that interference was justified from the perspective of Article 8, ECHR.[158]

Moreover, over time, the Court's increasing emphasis upon individual protection has resulted in a transformative effect on EU data protection. Reflecting a broader trend of the CJEU's greater role as a fundamental rights adjudicator,[159] consideration of the free market aims have been largely ignored by more recent CJEU cases. Rather, we see frequent statements that the objective of the Data Protection Directive is "to guarantee a high level of protection of personal data throughout the European Union", without having any regard at all to the explicit dual aims of the Data Protection Directive.[160]

One way in which we can see this transformative effect is in the interpretation of key threshold concepts, on the territorial and material application of data protection law. Confronted with cross-border data processing, the CJEU has expanded the territorial reach of EU data protection law, and the powers of data protection authorities. While the GDPR has explicit extra-territorial provisions,[161] the same was not the case under the Data Protection Directive, which was contingent on a controller engaged in processing "in the context of the activities of an establishment of the controller on the territory of the Member State." This requirement was interpreted expansively across a series of cases. The "establishment" criterion was to be interpreted in order to ensure protection of fundamental rights and freedoms,[162] which led in *Google Spain* to the finding that Google Inc., the ultimate US parent company of the Google group of companies, was deemed to be subject to the Data Protection Directive.[163] The reasoning of this case informed the determination of intra-EU powers in a series of cases about the capacity of national DPAs to exercise their authority across national borders. In *Weltimmo,* the Hungarian data protection authority was deemed to be competent over a Slovakian company,[164] the CJEU again emphasising that "establishment" should be understood broadly in light of the objective of protecting fundamental rights and freedoms of natural persons.[165] This reasoning has been extended to allow the application of multiple national data protection laws to the activities of a single data

---

[157] Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* [2003] ECR I-5014, para 68.
[158] ibid para 72.
[159] Gráinne de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20 Maastricht Journal of European and Comparative Law 168.
[160] E.g. C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 53; C-507/17 *Google v CNIL* (ECLI:EU:C:2019:772), para 54; C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601), para 61; Case C-132/21 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECLI:EU:C:2023:2) para 42. These latest two decisions have led Dreschler to question whether the CJEU is engaging in a judicial reinterpretation of the GDPR's objectives. Laura Drechsler, 'Did the Court of Justice (Re-)Define the Purpose of the General Data Protection Regulation?' (*CITIP blog*, 14 February 2023) <https://www.law.kuleuven.be/citip/blog/did-the-court-of-justice-re-define-the-purpose-of-the-general-data-protection-regulation/> accessed 20 February 2023.
[161] Article 3(2), GDPR.
[162] C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 53.
[163] ibid, paras 55-60.
[164] C-230/14 *Weltimmo* (ECLI:EU:C:2015:639).
[165] Therefore, the concept of establishment extended "to any real and effective activity – even a minimal one – exercised through stable arrangements." ibid, para 31.

controller.[166] In this way, the interpretation of a measure intended to have both free movement and fundamental rights aims in light of only the second aim has arguably frustrated the first. The CJEU's purported intention to ensure "effective and complete protection" of individuals has justified the application of multiple national versions of the Data Protection Directive, which was intended to act as a measure of harmonisation.

To some extent, more recently, the Court has had to try and contain its expansionism, when faced with the practical implications of that expansion. In *Google France v CNIL,* the CJEU once again considers the objective of the Data Protection Directive and GDPR and the importance of ensuring a high level of protection of personal data.[167] But the CJEU draws a limit to that objective, considering the global nature of the internet[168] and the impact on access to the information, and need to balance these interests,[169] determining that the de-referencing to be conducted in response to the right to be forgotten need only extend to the territory of the EU.[170] Thus, even where central to the assessment, the aim of individual protection is not absolute.

This expansive tendency seen in the territorial cases has also been seen in a series of cases on the material application of EU data protection law, including a broad interpretation of the concept of the data controller[171] and a narrow understanding of the exemptions from data protection law,[172] and a broad understanding of the types of data are captured by the regime as "personal data" is seen.[173] In each instance, the CJEU expressly links the need to adopt a broad interpretation of the relevant terms with the desire to ensure protection of individuals' data protection rights.

Thus, the Court's focus upon the objective of individual protection has shaped the expansion in scope of EU data protection law. It has also impacted the application of the regime, as other central concepts have also been interpreted in light of the objective of the protection of individuals.[174] In this way, the CJEU's heavy reliance on purposive interpretation of the legal regime in light of goal of protecting individuals illustrates both the status and impact of the individual as the normative foundation of EU data protection law.

---

[166] See C-191/15 *Verein für Konsumenteninformation* (ECLI:EU:C:2016:612) wherein the CJEU accepted that Amazon EU might have establishments in both Luxembourg and Germany and would therefore be subject to both Luxembourg and Germany's national data protection laws. In C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388) the CJEU confirmed that Facebook Inc. might be subject to the application of both Irish and German data protection laws, on the basis that it had an establishment in each jurisdiction over whom the relevant data protection authorities might exercise their competence, pars 45-64.

[167] C-507/17 *Google v CNIL* (ECLI:EU:C:2019:772), para 54.

[168] ibid, para 56.

[169] ibid, paras 57-67.

[170] ibid, para 73.

[171] C-131/12 *Google Spain and Google* (ECLI:EU:2014:317); C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388)*;* C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551);C-40/17 *Fashion ID* (ECLI:EU:C:2019:629).

[172] In a line of cases: C-101/01 *Bodil Lindqvist* [2003] ECR I-12992; C-212/13 *Ryneš* (ECLI:EU:2014:2428)*;* C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551).

[173] See section 3.2(a) below.

[174] For instance, the requirement of independence of national DPAs (C-518/07 *Commission v Germany* [2010] ECR I-01885, para 23) and the creation of a sui generis 'right to be forgotten' applicable to search engines (C-131/12 *Google Spain and Google* (ECLI:EU:2014:317) para 81.

3. The individual as a legal subject of data protection law

Beyond serving as the normative foundation, the individual is also a central legal subject of data protection law, as they are invested with legal status, rights and powers. In this sense, as the primary legal subject of data protection law, data protection law is ordered around the protection of the individual; first as a rights-holder, second, as the "data subject", third, as an affected natural person and fourth, at times as a data controller.

3.1. Rights-holder

The individual is confirmed as a rights-holder, who enjoys the right to the protection of their personal data, under Article 16 TFEU and Article 8 of the Charter, interpreted in light of Article 8 ECHR. We have seen how this right has significance to the legislative and judicial approach to data protection. Alongside this role, the creation of a new category of rights-holder has had another important legal effect, as the individual can now assert their right in legal claims beyond reliance upon data protection legislation. We see this in two senses, first, as the rights-holder brings their right to be weighed against other rights and interests in the application of other substantive areas of EU law, and second, as the individual can assert their right to data protection to challenge the legality of EU and national legal instruments.

The individual rights-holder's assertion of their right to data protection has had effect beyond the confines of traditional data protection cases. By way of example, in *Safe Interenvíos,* the CJEU was called upon to interpret a piece of national money laundering legislation.[175] The Court, in applying a proportionality analysis to that legislation, determined that the proportionality of the customer due diligence requirements in that legislation depended on the extent to which those measures intrude upon other rights and interests protected by EU law, such as the protection of personal data.[176] Thus, the status of data protection as a Charter right allows it to be a source of review or challenge in the field of money laundering legislation. This has been repeated in the recent *Luxembourg Business Registers* case in which part of a anti-money laundering Directive was invalidated by the CJEU on the basis of disproportionate interference with the rights to privacy and data protection of the underlying beneficial owners named on a public register on beneficial ownership.[177]

The right to data protection has had particular influence in a series of copyright infringement cases, wherein the CJEU has emphasised the need for the right to be data protection be weighed in "fair balance" with other competing interests. In *Promusciae,* concerned with the disclosure of subscriber details in order to facilitate infringement actions, the CJEU emphasised that copyright protection "cannot affect the requirements of the protection of personal data."[178] Rather, the multiple Charter rights engaged (the right to property under Article 17, the right to a remedy under Article 47, and the rights to data protection and respect for private life) must be reconciled and a fair balance between them struck.[179] In this way, the breadth of the obligation to facilitate copyright infringement action was contained—the telecommunications provider was under no obligation to communicate subscriber details

[175] C-235/14 *Safe Interenvios* (ECLI:EU:C:2016:154).
[176] ibid, para 109.
[177] Joined cases C-37/20 and C-601/20 *WM, Sovim SA v Luxembourg Business Registers* (ECLI:EU:C:2022:912).
[178] C-275/06 *Promusicae v Telefónica de España* [2008] ECR I-00271, par 57.
[179] ibid, para 68.

to copyright holders or their agents. Similar approaches were seen in *LSG*,[180] in *Scarlet Extended,*[181] *SABAM,*[182] and *Bonnier Audio and Others*.[183] In this way, the consideration of the impact upon the individual rights-holder has shaped the acceptable form of copyright injunction that copyright holders may obtain in accordance with EU law.

The individual's status as a rights-holder has also enabled challenges to be brought to the legality of EU legal instruments. An early challenge relying on Article 8 of the ECHR to challenge an action by the Council was rejected in *D and Sweden v Council,* wherein a refusal to pay a household allowance to an official in a same in a registered same sex partnership was not deemed to constitute an interference in private or family life.[184] However, in recent years, Article 8 of the Charter has become an important independent tool of challenge, usually considered in conjunction with the right to respect for private life under Article 7. A body of decisions have arisen since 2010, which have seen such challenges brought on the basis of the Charter and many succeed.

In *Schecke,* a section of common agricultural policy legislation was invalidated, on the basis that the disclosure rules relating to beneficiaries of the policy were incompatible with Articles 7 and 8 of the Charter.[185] The rules in question were held to fail a proportionality analysis,[186] and while acknowledging the validity of the objective of transparency underscoring the relevant rules, the Court emphasised that "[n]o automatic priority can be conferred on the objective of transparency over the right to protection of personal data..., even if important economic interests are at stake."[187]

Article 8 has had a particular impact upon instruments which were intended to limit data protection in the name of safeguarding security, and in these cases we see the limits of the individual rights asserted, as the right to data protection is weighed against state security and defence objectives. In *Schwartz* and *Willems,* a Council Regulation concerning the use of biometrics in travel documents was challenged.[188] Each rights-holder sought to argue that they ought not to be refused a passport for a refusal to submit biometric details to the issuing authority. In *Schwartz,* the CJEU ultimately deemed that the interference with Article 8 was lawful, while emphasising that Article 8 must be interpreted in relation to its function in society, and that the objective of the Regulation – to prevent illegal entry into the European Union, was an objective of general interest recognised by the union.[189] This determination

---

[180] C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* [2009] ECR I-01227, para 28.
[181] C-70/10 *Scarlet Extended* [2011] I-11959.
[182] C-360/10 *SABAM* (ECLI:EU:C:2012:85).
[183] C-461/10 *Bonnier Audio and Others* (ECLI:EU:C:2012:219).
[184] Joined cases C-122/99 P and C-125/99 P *D and Sweden v Council* (ECLI:EU:C:2001:304). The CJEU rejected the argument that there was a violation of Article 8, in a rather narrow reading of the right compared to contemporary approaches, finding that the refusal "only concerns the relationship between the official and his employer, does not of itself give rise to the transmission of any personal information to persons outside the Community administration. The contested decision is not therefore, on any view, capable of constituting interference in private and family life within the meaning of Article 8 of the [ECHR]." Ibid, paras 59-61.
[185] C-92/09 *Volker und Markus Schecke and Eifert* [2010] I-11063.
[186] ibid, para 76.
[187] ibid, para 85.
[188] Council Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents. C-291/12 *Schwartz* (ECLI:EU:C:2013:670)*;* Joined cases C-446/12 to C-449/12 *Willems and Others* (ECLI:EU:C:2015:238).
[189] C-291/12 *Schwartz* (ECLI:EU:C:2013:670), para 33, paras 37-38.

was followed in *Willems,* and the Court said that the use of biometrics under the Regulation had already been deemed compatible.[190]

Perhaps the most striking impact of Article 8 has been a series of cases in which the individual right to data protection has been the basis (or partial basis) upon which the CJEU has judged the entirety of legislative instruments, in accordance with compatibility with the protections of Article 7 and 8. The first case, *Digital Rights Ireland,* saw the CJEU invalidate the Data Retention Directive[191] due to its disproportionate impact on Articles 7 and 8.[192] The Court showed awareness of the oppressive nature of surveillance regimes, noting that the retention regime would be "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[193] A regime providing for generalised data retention was considered to be a wide-ranging and "particularly serious" infringement.[194] While interferences with Article 8 can be justified under Article 52(1) of the Charter, this regime was deemed disproportionate and invalidated in its entirety. As a determination of the reach of the right to data protection, *Digital Rights Ireland* is striking in how expansively the CJEU construed the right and the determination that "the EU legislature's discretion is reduced" due to the important role of the protection of personal data and the seriousness of the infringement.[195]

Similar approaches have subsequently been seen in a number of cases. In *Schrems,* we saw the invalidation of a Commission adequacy decision, which had legitimised certain data transfers from the EU to the US.[196] While the actual invalidation of the decision was on a somewhat formalistic basis,[197] the standards for a valid adequacy decision set out by the CJEU were deeply informed by a fundamental rights orientation.[198] In the *PNR* decision, a proposed international agreement facilitating the sharing of passenger name records between EU and Canada, was found not to comply with the Charter.[199] In *Tele2,* we see the Court assess the legality of national surveillance measures against the requirements of the Charter, and once again finding the regimes lacking.[200] Once again, in *Schrems II,* the Privacy Shield adequacy decision[201] and the Standard Contractual Clauses[202] which can

---

[190] Joined cases C-446/12 to C-449/12 *Willems and Others* (ECLI:EU:C:2015:238), par 46.
[191] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105/54, 13/4/2006, p54-63).
[192] Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238).
[193] ibid, para 37.
[194] ibid, para 37.
[195] ibid, para 48.
[196] C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650).
[197] The Court emphasised that the Commission had failed to formally state that the US in fact ensured an adequate level of protection, and invalidity followed from this absence of a formal determination. Ibid, paras 97-98.
[198] For example, the Court establishes a test for adequacy is that of protection "that is essentially equivalent to that guaranteed within the European Union by virtue of [the Data Protection Directive] read in light of the Charter." Para 73.
[199] Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656).
[200] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970).
[201] COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (OJ 2016 L 207, p. 1.)
[202] COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European

legitimise data transfers out of the European Economic Area were considered against the standards of Articles 7 and 8 of the Charter.[203] The Standard Contractual Clauses survived this scrutiny, but the Privacy Shield decision was deemed to be incompatible with the protections required, due to the disproportionate interference possible with the rights to data protection and respect for private life under US surveillance laws. In *Ligue des droits humains* the Passenger Names Record Directive was interpreted restrictively so that it might survive a challenge on the basis of the rights to data protection and respect for private life.[204]

This series of cases demonstrate the potency of the individual's right to data protection, often wielded alongside the right to respect for private life, as a source of review for EU and national legislative measures. The individual, and their status as a protected rights-holder, is central to these determinations, often as the initiator of these actions, and as the weighing of competing interests must be balanced against the impact on the individual.

3.2. Data subject

The individual also attains a new legal status within the legislative data protection scheme under the GDPR and its predecessor, the Data Protection Directive. As the protected subject of this regime—the "data subject"—the individual is central to the logic and functioning of this legislative scheme.

As I shall explain, the concept of the individual and their data determines the scope of this regime, and the legality of data processing thereunder is often (though not always) judged by reference to the individual.

(a) The scope of the GDPR is defined in terms of the individual

Two related concepts are central to the scope of the GDPR and, before it, the Data Protection Directive: the data subject and personal data.

The GDPR defines its material scope by way of the concept of personal data. The GDPR applies "to the processing of personal data wholly or partly by automated means."[205] Processing is a very broad concept, entailing any use (including collection)[206] and therefore more attention has focussed on "personal data" as a threshold concept. The first question in any data protection analysis thus tends to be—is the data in question "personal data"?[207]

Personal data, in turn, is defined in terms of an individual: a living natural person.[208] In order to qualify as personal data, the data must relate to an individual–the "data subject"–who must be identified, or identifiable.

Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by COMMISSION IMPLEMENTING DECISION (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

[203] C-311/18 *Facebook Ireland & Schrems* (ECLI:EU:C:2020:559).

[204] C-817/19 *Ligue des droits humains* (ECLI:EU:C:2022:491).

[205] Article 2(1), GDPR.

[206] Article 4(2), GDPR.

[207] We see this in a number of CJEU decisions, including determinations that the following types of data are personal data: IP addresses (C-360/10 *SABAM* (ECLI:EU:C:2012:85)*);* fingerprints (C-291/12 *Schwartz* (ECLI:EU:C:2013:670)*);* records of working time from a time clock system (C-342/12 *Worten* (ECLI:EU:C:2013:355); evidence gathered by private detectives (C-473/12 *IPI* (ECLI:EU:C:2013:715)); video surveillance (C-212/13 *Ryneš* (ECLI:EU:2014:2428)); tax ID numbers (C-496/17 *Deutsche Post* (ECLI:EU:C:2019:26)).

[208] Article 4(1) provides (in part) "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly".

This question of when data is sufficiently related to an individual, and whether an individual is identifiable is somewhat ambiguous on the face of the legislation.[209] Unsurprisingly, therefore there have been a series of referrals to the CJEU on the meaning of personal data. The Court's approach has seen some change over time, with a general tendency towards a more expansive understanding of the concept.

In *YS and Others,* the CJEU was asked whether a legal analysis concerning applicants for residence permits was personal data.[210] The Court determined that while such a legal analysis might contain personal data, it was not in itself personal data.[211] The Court's interpretation was guided by the function of personal data in an access request (which the applicants had been denied).[212] The Court emphasised that the right of access was intended to enable the exercise of other procedural rights (such as rectification, or to check the accuracy of that data),[213] and that the Data Protection Directive was not intended to provide a right of access to administrative documents more generally.[214]

By contrast, the later cases of *Breyer*[215] and *Nowak,*[216] moved away from this instrumental approach linked to the right of access.[217] In *Breyer,* the CJEU considered whether dynamic IP addresses were personal data, in circumstances where a website operator would need to obtain data from a third party in order to identify the underlying individual.[218] The CJEU confirmed a relative vision of personal data. A controller need not hold all the information enabling the identification of the data subject, if by means reasonably likely to be used, a combination of the data would rendering the individual identifiable.[219] The possibility for the website operator to contact the relevant third party (the internet services provider) was deemed to be means reasonably likely to be used.[220] In *Nowak,* the CJEU was called upon to determine whether an examination script was personal data, after an applicant who sought access to his script after a series of failed accountancy examinations.[221] Determining that the script was personal data, the Court took a very expansive approach. The CJEU expressly determined that a broad approach to the concept of personal data was appropriate, finding that the use of the expression "any information" in the definition of

---

[209] See Purtova, 'From Knowing by Name to Targeting' (n 86).
[210] Joined cases C-141/12 and C-372/12 *YS and Others* (ECLI:EU:C:2014:2081).
[211] ibid, para 39.
[212] ibid, para 44.
[213] ibid, para 44.
[214] ibid, para 45-46.
[215] C-582/14 *Breyer* (ECLI:EU:C:2016:779).
[216] C-434/16 *Nowak* (ECLI:EU:C:2017:994).
[217] *Nowak* seems at odds with the earlier *YS* decision, though the Court presents them as compatible, on the basis that the ability to obtain the examination script served the purpose of the Data Protection Directive in guaranteeing the protection of the candidate's data. The implication seems to be that the migrant applicant in *YS* on the other hand sought access to his data to review the decision making by the public authority, rather than to safeguard his data protection. This positioning by the CJEU seems unconvincing (surely *Nowak* was interested not only in his data protection, but in improving his examination results) and conflates the rights to privacy and data protection in its reasoning. A number of scholars have commented on the unclear nature of the status of *YS.* (Benjamin Wong, 'Delimiting the Concept of Personal Data after the GDPR' (2019) 39 Legal Studies 517, 526. Orla Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 International Journal of Law in Context 162. Lee A Bygrave and Lee Tosoni, 'Article 4(1). Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 110.)
[218] C-582/14 *Breyer* (ECLI:EU:C:2016:779).
[219] ibid, pars 43-49. See also, Recital 26, Data Protection Directive.
[220] ibid, para 48.
[221] C-434/16 *Nowak* (ECLI:EU:C:2017:994).

personal data "reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective… provided that it 'relates' to the data subject."[222] In turn, the test provided for whether information "relates to" the data subject is also wide in scope, extending to information which "by reason of its content, purpose or effect, is linked to the data subject."[223] It is unsurprising, therefore, that the CJEU determined that the examination script and examiner's comments were to be regarded as personal data, attracting the full suite of data protection obligations and rights.[224]

The resulting standard of personal data is very broad, post-*Nowak*. The Court has effectively endorsed the theory that breadth in protection results in greater protection, though this has been subject to criticism.[225] Any data which touches or might touch on the individual experience comes to be subject to the GDPR, and therefore the threshold for the application of the data protection law is contingent on an analysis of the relation of that data to an individual.

(b) The legality of data processing is usually judged by reference to the individual

In order for data processing to be lawful under the GDPR, two general requirements must be met. First, the controller must be able to demonstrate that it has a lawful basis for that processing.[226] As I shall explain, the individual is central to the assessment of legality of each, though not the exclusive consideration. Second, the controller must comply with the data protection principles.[227] These principles take a less individually oriented approach.

As a pre-condition to data processing, the data controller must be able to justify their processing on one of six conditions. Three we might describe as individually-oriented, two have a public-orientation and the final legal basis is a hybrid, considering multiple parties.

Three legal pre-conditions explicitly invoke consideration of the individual, the data controller may adduce: the data subject's consent, necessity for the performance of a contract with the data subject, and necessity for the protection of the data subject's (or another natural person's) vital interests.[228] Consent has long been considered fundamental to data protection law,[229] and it is the sole legal pre-condition named in the fundamental right to data protection.[230] However, the GDPR has tightened the ability of controllers to rely on an individual's consent,[231] because of a concern that divergent implementations of consent

---

[222] ibid, para 34.
[223] ibid, para 35.
[224] ibid, para 47.
[225] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 87); Dalla Corte (n 87).
[226] Article 6, GDPR.
[227] Article 5, GDPR.
[228] Article 6(1)(a), 6(1)(b), 6(1)(d), GDPR.
[229] See for example, Eleni Kosta, *Consent in European Data Protection Law* (Brill 2013); Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution*, vol 526 (Springer International Publishing 2018) <http://link.springer.com/10.1007/978-3-319-92925-5_8> accessed 25 August 2021; Bietti (n 86).
[230] Article 8(2) of the Charter provides: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."
[231] See Article 7 which adds conditions to consent, and Article 8 which adds conditions to the applicability of children's consent in relation to information society services.

across Member States were resulting in poor consent practices.[232] The Court has also recognised that concept of consent cannot be given an overly expansive interpretation—in *Schwartz*[233] and in *Planet 49*.[234]

Two pre-conditions have a public orientation. The controller may lawfully process data where the processing of that data is necessary for compliance with a legal obligation, or where the processing is necessary for the performance of a task carried out in the public interest.[235] While we might characterise these analyses as a weighing of public concerns, in fact the impact upon the individual is still relevant to the consideration of these pre-conditions. This is because any public legislative measure which represents an interference with the right to personal data—any legislative measure which involves data processing and therefore might satisfy either the legal obligation or public interest ground—is subject to review in terms of interference with the right to data protection. Thus, even if processing is nominally justified under Article 6 of the GDPR under a piece of national or EU legislation, such a measure may be subject to a second tier of legal challenge on the basis of the interference with the individual's fundamental right to data protection under Article 8 of the Charter. We see this applied in a number of cases before the CJEU. In *Manni,* the CJEU considered that the processing of data for the purposes of the publication of a statutory companies register could be justified by a number of legal bases, including compliance with a legal obligation and public interests.[236] Nevertheless, in order to satisfy itself that this reliance on these pre-conditions was legally appropriate, the CJEU went on to analyse whether the interference with the fundamental rights of concerned persons, ultimately determining that while there was an interference it was not disproportionate.[237] Similarly, in *Puškár,* the CJEU considered that data collection and processing in order to collect taxes and combat tax fraud would be lawful under the public interest ground, provided that the national legislation in question satisfied a proportionality analysis.[238] This approach was confirmed in the recent *OT* decision, as the CJEU confirmed that the requirement that measures based on public interest or legal obligation meet an objective of public interest and be proportionate[239] is an expression of the requirements under Article 52(1) of the Charter.[240]

Finally, a controller may justify its processing on the basis that the processing is necessary for the purposes of the legitimate interests of the controller or a third party.[241] However, this legitimate interest must not be overridden by the interests or fundamental rights and

---

[232] Eleni Kosta, 'Article 7. Conditions for Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 347.
[233] The CJEU recognised that an individual could not consent to the inclusion of personal data on their passport, as it was essential to own a passport. C-291/12 *Schwartz* (ECLI:EU:C:2013:670), para 31.
[234] The Court emphasised the need for consent to be unambiguous and required active behaviour by the individual, and therefore pre-ticked boxes could not be relied upon. C-673/17 *Planet49* (ECLI:EU:C:2019:801), para 65.
[235] Article 6(1)(c), 6(1)(e) GDPR.
[236] C-398/15 *Manni* (ECLI:EU:C:2017:197), para 42.
[237] ibid, para 56.
[238] C-73/16 *Puškár* (ECLI:EU:C:2017:725), pars 102-117.
[239] Per Article 6(3), GDPR.
[240] The CJEU found that "Article 6(3) of the GDPR specifies, in respect of those two situations where processing is lawful, that the processing must be based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued. Since those requirements constitute an expression of the requirements arising from Article 52(1) of the Charter, they must be interpreted in the light of the latter provision and must apply mutatis mutandis to Article 7(c) and (e) of Directive 95/46." Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601), para 69.
[241] Article 6(1)(f), GDPR.

freedoms of the data subject.[242] As explained in *Rīgas,* this involves a three stage analysis.[243] First, a legitimate interest pursued by the data controller or by third parties must be established. Second, it must be necessary to process the data for the purposes of that legitimate interest. Third, the fundamental rights and freedoms of the data subject must be considered, to determine if they take precedence over the legitimate interest pursued.

Therefore, while the six legal pre-conditions to processing might appear to have different orientations, nevertheless the consideration of the individual and their interests is central to each. Moreover, for certain types of individuals, particularly children and vulnerable persons, additional rules are implemented before data may be lawfully processed.[244]

By contrast, the data protection principles are less explicitly tied to the individual. Indeed, only two of the data protection principles are defined by reference to the data subject. First, the lawfulness, fairness and transparency requirement is assessed 'in relation to the data subject',[245] though the requirement of fairness in Article 8 is not so tied to the subject.[246] Second, the storage limitation principle requires that personal data is kept in a form which permits identification of data subjects no longer than is necessary for the purpose of processing.[247] On the other hand, the purpose limitation requirement, data minimisation, data accuracy and integrity and confidentiality principles are all expressed generally, without using the data subject as a focus of the principle.[248] Accordingly, while there is a link to the individual data subject, many of the principles provide for general principles of data governance, which might be said to benefit all data subjects, rather than judging by individualised standards. These principles ensure a basic set of standards with which data controllers must abide, and in setting standards which limit data controller's freedom to impact persons.[249]

The individual's status as this protected subject of data protection law is characteristic of the individual's centrality to the regime. It is the logic of individual protection which primarily informs the legislative provisions in their design and application. Nevertheless, these provisions are not exclusively individualistic, as other parties (controllers, other affected natural persons, the state) and interests may come to be weighed in the ultimate balance.

3.3. Other natural persons?

The third category of protected subject which we encounter in data protection law is that of "other natural persons." We have seen how in cases considering the right to data protection, that right must often be balanced against the rights and interests of others.[250] In addition to

---

[242] ibid.
[243] C-13/16 *Rīgas satiksme* (ECLI:EU:C:2017:336), para 28.
[244] Article 8, 24, GDPR. See also Eva Lievens and Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 269; Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law & Security Review 105415.
[245] Article 5(1)(a), GDPR.
[246] Article 8(2) provides (in part): "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*."
[247] Article 5(1)(e), GDPR.
[248] Articles 5(1)(b), (c), (d) and (f). Though Purtova has connected purpose limitation with individual informational self-determination. Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86).
[249] Lynskey has suggested that these principles offer an opportunity to "shift away from the individual-centric approach crystalized in other parts of the GDPR. Orla Lynskey, 'Delivering Data Protection: The Next Chapter' (2020) 21 German Law Journal 80, 83.
[250] See section 3.1 above.

these other affected parties, EU data protection legislation sometimes confers legal status on other natural persons. In various provisions of the law, other affected natural persons attract a variety of protections, in a piecemeal and inconsistent fashion.

The GDPR acts to protect or accommodate the interests and rights of other natural persons (separate to the envisaged data subject) in a number of provisions. The manner in which the data subject is conceived of in relation to others is considered in further detail in Chapter 4, but for the purposes of this chapter, I consider how individuals other than the relevant data subject are recognised and protected by EU data protection law.

This extension of protection to persons beyond the data subject does not occur in any particularly consistent or considered approach, but rather incidentally. In the delineation of a number of the GDPR's provisions, other natural persons come to be given legal protection. We see the explanation for the inclusion of these interests at the outset of the GDPR, as the right to data protection is recognised to be a relative rather than absolute right, and must be balanced against other rights.[251]

Other natural persons, as protected subjects, then recur in a number of the provisions of the GDPR, as their interests are to be accommodated. The provisions echo the language of Article 52(1) of the Charter, which allows for the limitation on the exercise of Charter rights, *inter alia* where necessary "to protect the rights and freedoms of others".[252]

For example, within the legal bases for processing, the vital interests "of another natural person" might justify processing.[253] In some of the data subject rights, the interests of another natural person must be weighed. The right to data portability acknowledges the possibility of another affected data subject whose interests must be considered.[254] The right to access and the right to data portability are not to "adversely affect the rights and freedoms of others."[255] The right to objection may be overruled where the continued processing of restricted data is "for the protection of the rights of another natural or legal person".[256] In addition, Member States may restrict the obligations upon controllers by national law, where necessary to safeguard "the rights and freedoms of others."[257]

Thus, we see that the recognition of other affected parties is inconsistent. For example, some of the legal bases, some of the data subject rights make such reference, but not all. The potential impact upon other natural persons is not always included in provisions where such impact might occur. One curious example is seen in the legitimate interests basis for processing. This basis explicitly adopts a balancing test between the need for processing (the legitimate interests of the controller or of a third party) and the fundamental rights and freedoms to be protected (that of the data subject only).[258] Thus another natural person who

---

[251] Recital 4 of the GDPR provides (in part): "The right to the protection of personal data is not an absolute right: it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."
[252] Article 52(1), Charter.
[253] Article 6(1)(d), GDPR, and Article 9(2)(c), GDPR for sensitive personal data.
[254] Recital 68, GDPR provides: "Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation."
[255] Article 15(4) and Article 20(4), GDPR. Recital 63, GDPR elaborates regarding access, referring to the trade secrets, intellectual property and copyright of others.
[256] Article 18(2), GDPR.
[257] Article 23(1)(i), GDPR.
[258] Article 6(1)(f), GDPR: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or

has an interest in processing is acknowledged, but one who has an interest against processing is not. This suggests a particularly individualistic understanding of data protection harms. Thus, we see occasional mentions of the potential impact upon the rights or freedoms of others, but without any coherent logic to where such provision is included and where not.

3.4. The individual as a responsible subject: the data controller

Alongside the individual's role as a protected subject, the individual may also be a responsible subject under the GDPR. The term of art for the regulated subject under the GDPR is the "data controller."[259] As shall be explained, while it does not seem that the individual was originally intended to be legally responsible for ensuring compliance with the data protection regime, this was always theoretically possible. Moreover, individuals being classified as data controllers is increasingly likely due to the CJEU's broad interpretation of the concept of controller and narrow interpretation of the purely personal and household processing exemption, as shall be explored below.

The data controller, as the entity which determines how and why data is to be processed, is charged with demonstrating the legality of that processing. The controller is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[260] The data controller's responsibility for demonstrating compliance with the GDPR's obligations is enshrined in the principle of accountability.[261] In other words, the controller must not only adopt appropriate measures to ensure lawful processing, but also be able to demonstrate this lawfulness.[262] This responsibility is further articulated in the proactive obligations upon the data controller: to ensure that data protection measures are integrated into the data processing from the outset (data protection by design), and that the most protective settings are adopted by default (data protection by default).[263]

The controller is also subject to a series of more specific bureaucratic obligations. The data controller must satisfy transparency obligations by providing an extensive amount of information to data subjects.[264] The data controller must also facilitate the exercise of the data subject's procedural rights, subject to the terms of those rights: providing access to data,[265] rectifying inaccurate data upon request,[266] erase personal data[267] or restrict it[268] in

---

fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[259] The 'data processor' is the second category of regulated entities. Processors engage in data processing on behalf of the controller, but have a smaller range of independent responsibilities. For the purpose of this chapter, I focus on the data controller rather the data processor. I do this for two reasons; first, the controller is the entity with the majority of the compliance regulations under the GDPR, and second, the concept of the data processor has not yet been explored in the case law of the CJEU in a manner that would suggest an increased role for individuals.

[260] Article 4(7), GDPR.

[261] Article 5(2), GDPR. Article 24(1), GDPR provides: Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

[262] The principle of accountability is considered further in Chapter 5, section 5.2.

[263] Article 25, GDPR.

[264] The information prescribed is set out in Articles 13 and 14, GDPR.

[265] Article 15, GDPR.

[266] Article 16, GDPR.

[267] Article 17, GDPR.

certain cases, and facilitate the exercise of the right to data portability.[269] The data controller must also maintain detailed records of processing activities, which must be available to data protection authorities for inspection.[270] The data controller is also charged with maintaining appropriate security measures to keep personal data secure.[271] In cases where such security measures fail or are circumvented, and there is a data breach, the data controller is under notification obligations.[272] In advance of new high risk data processing projects, the data controller must engage in due diligence and conduct a data protection impact assessment, which may involve consultation with data subjects or the data supervisory authorities in certain cases.[273] Certain data controllers must appoint data protection officers.[274]

The structuring of these obligations is aligned with an institutional or bureaucratic vision of the controller. A number of scholars have observed such tendencies in the concept of the controller. Both Reed and Van Alsenoy have pointed to the embedding in the Data Protection Directive of assumptions about the nature of controllers based on the prevailing institutional data processing practices of the 1970s.[275] The controller concept, Reed argues presumes a certain type of organisational structure, observing "an implicit assumption that there is central control of personal data processing and that the organisation's staff merely undertake that processing in accordance with central instructions."[276] While Reed is focussed on the designation of responsibility between employers and individual employees, his observation also resonates with the model of regulation we see. The nature of controllers' compliance obligations: record keeping, notifications, drafting transparency obligations, complying with access requests etc. presume a certain measure of bureaucratic capacity and organisational resources. Similarly, Bygrave has observed in the context of the obligations of data protection by design and default that "the GDPR seems to assume that controllers will have the necessary power to steer the market and technology foundations for information systems development in a privacy-friendly direction."[277] A regime which Purtova characterises as "highly intensive"[278] seems to presume that controllers are commercial, institutional or bureaucratic entities, if controllers are to ever be able to meaningfully comply with their obligations.

However, that is not the legal position. There is no limitation as to which types of persons might be considered controllers. From the outset, the definition of a data controller makes it clear that either legal or natural persons might be controllers.[279] And as we shall see, a series of decisions of the CJEU suggest an increased role for individuals as controllers.

---

[268] Article 18, GDPR.
[269] Article 20, GDPR.
[270] Article 30, GDPR.
[271] Article 32, GDPR.
[272] Articles 33 and 34, GDPR.
[273] Articles 35 and 36, GDPR.
[274] Article 37, GDPR.
[275] Brendan Van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25. Chris Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation' [2007] Journal of Information, Law and Technology 33.
[276] Reed (n 250) 9.
[277] Lee A Bygrave, 'Data Protection by Design and by Default' [2022] Oxford Online Encyclopaedia of European Union Law para 25 <https://ssrn.com/abstract=3944535>.
[278] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86) 42.
[279] Article 4(7), GDPR.

The increased designation of individuals as data controllers has arisen due to a series of cases, which has done three things in parallel. This trend has been observed by a number of scholars.[280] First, the purely personal and household exemption has been narrowed to extremely limited application. Second, the concept of "controller" has been interpreted expansively. And third, the concept of "joint controllers" has been expanded. These three developments shall be examined in turn, and the consequence examined: an increased legal determination that individuals are to be considered data controllers.

Processing which is carried out "by a natural person in the course of a purely personal or household activity" is exempted from the GDPR.[281] However, there have been a series of cases involving natural persons before the CJEU in which the scope of this exemption (hereinafter, the "household exemption") has been restricted. First, in *Lindqvist,* a catechist who maintained an internet page for parishioners preparing for their communion was not deemed to fall within the household exemption.[282] The household exemption, the CJEU clarified, extended only to activities "carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."[283] In *Ryneš,* the narrowing of the exemption continued, in a case concerning the capturing of video surveillance from a CCTV camera placed in the eaves of a family home.[284] The Court emphasised the objective underlying the Data Protection Directive, and took a purposive approach, determining that the objectives of protecting private life and data protection required the exemption to be narrowly construed.[285] The Court also noted that there was a basis for this narrow construction in the wording of the provision, emphasising the requirement that the processing is in the context of a *purely* personal or household activity.[286] Thus, any surveillance which captured any public space was deemed to be "directed outwards from the private setting of the person processing the data" and therefore outside the household exemption.[287] This reasoning reappeared in the *Jehovan todistajat,* where the Court emphasised that door to door preaching by members of the Jehovah's Witness Community was "directed outwards from the private setting of the members",[288] and because the data collected was being shared with other members of the community, this was deemed to be accessible "to a potentially unlimited number of persons".[289] The outcome of these cases is that the household exemption is very narrow, seemingly confined to one's private abode and limited to offline activities. Van Alsenoy has pointed to the *Lindqvist* and *Ryneš* judgments to argue that it is time to expand the household exemption, to avoid a disproportionate and impractical regulation of individual activities.[290] Indeed, in *Ryneš* the Court suggested that despite the application of the Data Protection Directive, the individual data processing in question might be justified by the legitimate interests of the data controller.[291] However, even if the processing itself might be lawful, the CJEU did not grapple

---

[280] Edwards and others (n 83); Chen and others (n 83); Finck (n 83).
[281] Article 2(c), GDPR.
[282] C-101/01 *Bodil Lindqvist* [2003] ECR I-12992.
[283] ibid, para 47.
[284] C-212/13 *Ryneš* (ECLI:EU:2014:2428).
[285] ibid, para 28-29.
[286] ibid, para 30.
[287] ibid, para 33.
[288] C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551), para 44
[289] ibid, para 45.
[290] Van Alsenoy (n 83) 35.
[291] In *Ryneš,* the CJEU noted that the legitimate interests of Mr Ryneš and his family could be taken into account. C-212/13 *Ryneš* (ECLI:EU:2014:2428), para 34.

with how Mr Ryneš or similar individuals might begin to satisfy the other myriad obligations of a data controller.

At the same time as the narrowing of the household exemption, the CJEU has been expanding the understanding of the term data controller. First, it has done so by emphasising that the concept of the data controller should be given a broad interpretation. In *Google Spain,* the CJEU held that the objective underlying the concept of a controller was "to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects".[292]

Drawing on this broad interpretation of the concept of the controller has subsequently informed the expansion of the concept of joint controllership. Joint controllership has always been a feature of the Data Protection Directive and the GDPR; after all the definition of the controller provides for a person who "alone or jointly with others, determines the purposes and means of processing of personal data."[293] Indeed, the GDPR introduced new provisions addressing the joint controllers and introducing a requirement that they arrange their respective responsibilities between themselves,[294] which customarily might be achieved by way of contract.

However, a series of recent decisions from the CJEU have expanded the notion of joint controllership, building on the determination in *Google Spain* that controllership should be interpreted broadly to ensure protection of data subjects. In *Wirtschaftakademie Schleswig-Holstein,* the CJEU was asked to consider the responsibility of the administrator of a Facebook fan page.[295] The CJEU found the administrator to be a joint controller, emphasising that this determination "contributes to ensuring more complete protection of the rights of persons visiting a fan page."[296] The administrator, the CJEU pointed out "by creating such a page, gives Facebook the opportunity to place cookies on the computer or device of a person visiting its fan page"[297] and some ability to define the parameters of the data processing, as they had an element of choice about the statistics generated by Facebook about page visitors.[298] In *Jehovan todistajat* such an approach was repeated, this case concerning the respective responsibilities of the Jehovah's Witness Community and individual members engaging in door-to-door preaching.[299] The CJEU determined that each were joint controllers, examining the role each played in the collection and use of the personal data. The individual members, decide in what circumstances to collect personal data, which specific data are collected and how those data are subsequently processed.[300] However, the Jehovah's Witness Community, the CJEU noted, organised, co-ordinated and encouraged its members to engage in the door-to-door preaching, and therefore was to be considered a joint controller with the members.[301] Indeed, the CJEU emphasised that a controller need not have access to all the relevant personal data concerned. It is a somewhat curious finding, as the characterisation of the role of the Jehovah's Witness Community seems very similar to what we might consider an employer – who determines the mission, and sets the activities to be carried out, and the members like employees – who

---

[292] C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 34.
[293] Article 2(d) Data Protection Directive; Article 4(7), GDPR. (My emphasis.)
[294] Article 26, GDPR.
[295] C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388).
[296] ibid, par 42.
[297] ibid, par 35.
[298] ibid, par 36.
[299] C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551).
[300] ibid, par 70.
[301] ibid, par 73.

determine how to achieve the mission, within the context of their daily duties. And yet, we would rarely consider employees to be independent data controllers or joint data controllers with their employers.[302] It seems likely that the Court was influenced by the *sui generis* nature of the Jehovah's Witness Community and its organisational structure, as well as the framing of the question – which focused not on whether the members were to be responsible, but whether the Jehovah's Witness Community was.

Despite criticism of the expanded use of the concept of joint controller by Advocate General Bobek in *Fashion ID,*[303] the CJEU continued in its approach. Fashion ID, a website operator, had embedded a Facebook Like button on its website (a social plugin which facilitates the provision of information about website visitors to Facebook). Fashion ID, the Court determined, was to be considered a joint controller. It emphasised Fashion ID's factual role to justify its responsibility; that that through the embedding of the social plugin Fashion ID had made it possible for Facebook to obtain the visitors' personal data.[304] Fashion ID was said to be fully aware of the fact that the social plugin served as a tool for the collection and disclosure of personal data of website visitors.[305] The placing of the plugin in the first instance played a "decisive influence" over the collection of the personal data in question.[306] The CJEU seems to have tried to carve out the responsibilities between the joint controllers; both controllers must be able to advance a legitimate interest to legitimise their processing[307] and both controllers would need to obtain consent as to the dataset and operations in respect of which that controller has actually determines the purposes and means.[308]

In an environment where online services have been dominated by a small number of platforms, who generally finance themselves through advertising, enabled through the deployment of tracking technologies, this series of cases would suggest an increased number of individuals may inadvertently find themselves regulated as data controllers. By using a free commercial service to host their blog, or fanpage or photograph collection, or using a connected device, an individual may be deemed to be exercising a "decisive influence" in the collection and transmission of data about others, such that by distribution to a potentially indefinite number of people, they will be subject to the full suite of obligations of a data controller under the GDPR.

4. Agent of data protection law

The individual is also an agent of data protection law. Connected to the individual's status as a data subject, the legal safeguarding of the individual's actions regarding their personal data is integral to the performance of data protection law. Though the exercise of informational decision making, the grant of procedural rights and the framing of the fundamental right to data protection, the individual is said to be empowered to perform data

---

[302] Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia Ltd 2019) 117–118.
[303] Advocate General Bobek deals with the issue at length, with particular concerns as to "the practical implications of such a sweeping definitional approach", noting that a lack of conceptual clarity as to who is the controller and with regard to what data, can lead "into the realm of actual impossibility for a potential joint controller to comply with valid legislation". C-40/17 *Fashion ID* Opinion of Advocate General Bobek 19 December 2018 (ECLI:EU:C:2018:1039) para 72, 84
[304] C-40/17 *Fashion ID* (ECLI:EU:C:2019:629), par 75.
[305] ibid, par 77.
[306] ibid, par 78.
[307] ibid, par 96.
[308] ibid, par 105-106.

protection.[309] While the individual is clearly not the only agent of data protection (accountable data controllers, data protection authorities, legislative and judicial authorities all also have roles to play), given the focus of this chapter, this section focuses on the individual's role in operationalising data protection. This role of the individual is seen at two phases of data protection. First, the individual is proactive – they may decide how their information is to be used. Second, the individual may act to defend their interest, in various ways.

4.1. The individual may decide how their information is to be treated

Informational self-determination, or the control of one's personal data is often written about (or indeed criticised) in the context of the Data Protection Directive and the GDPR.[310] After all, the principle of consent is core to the right to data protection, and one of the grounds upon which data processing is justified.

The two central ways in which the individual may be said to control their information is through two legal bases for data processing. Data processing may be legal if the data subject has consented to the processing in question,[311] or where the processing is necessary for the performance which a data subject has entered into with the controller.[312] It seems, in response to concerns about the circumstances in which individuals' consent was being relied upon,[313] in the current generation of data protection legislation, reliance on individual decision making has been limited. The GDPR places conditions on consent, in an apparent attempt to ensure individuals are not coerced into providing consent. The controller is now responsible for demonstrating that the data subject has consented.[314] Consents must be separated from other matters in a written declaration, and presented "in an intelligible and easily accessible form, using clear and plain language."[315] Perhaps most interestingly, the GDPR introduces what Peifer and Schwartz call a prohibition on "tying" consents.[316] By requiring that "utmost account" must be taken of whether performance of a contract is made conditional on a consent to non-necessary processing, the GDPR suggests such

---

[309] For this reason, Ausloos has linked these rights and control more broadly to the essence of the right of data protection. Ausloos (n 84) 61. See also Chapter 5 more generally.

[310] See e.g. Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009); Lynskey, *The Foundations of EU Data Protection Law* (n 86); Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 SCRIPTed <http://script-ed.org/?p=1927> accessed 6 November 2018; Tobias Matzner and others, 'Do-It-Yourself Data Protection—Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move*, vol 24 (Springer Netherlands 2016) <http://link.springer.com/10.1007/978-94-017-7376-8_11> accessed 21 March 2019; Woodrow Hartzog, 'Opinions · The Case Against Idealising Control' (2018) 4 European Data Protection Law Review 423; Bietti (n 86); Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia?' (2020) 9 Internet Policy Review <https://policyreview.info/articles/analysis/personal-information-management-systems-user-centric-privacy-utopia> accessed 13 January 2021; Lynskey, 'Delivering Data Protection' (n 249); Ausloos (n 84).

[311] Article 6(1)(a), GDPR.

[312] Article 6(1)(b), GDPR.

[313] See in particular Recitals 42 and 43, GDPR. There is emphasis on the requirement that consent is freely given.

[314] Article 7(1), GDPR.

[315] Article 7(2), GDPR.

[316] Karl-Nikolaus Peifer and Paul M Schwartz, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 143.

circumstances in which consent is tied to the performance of a contract will mean that the consent is not freely given.[317]

Therefore, the individual may be an agent of data protection law through the exercise of decision making as to how their data will be processed, legitimated through the doctrines of consent and contractual necessity. However, the limitation of consent seen under the GDPR and the emphasis of the high threshold of "necessity" which informs the contractual necessity ground should arguably increase our scrutiny over the extent to which decision making is truly a free exercise of agency or coerced.

4.2. The individual is equipped with rights it might use to safeguard their data

The individual is also an agent of data protection law through their exercise of a suite of data rights to defend their interests. First, individuals have a series of rights which they might exercise against data controllers, in order to ensure that their data is being processed lawfully by that controller. Second, the individual has a set of procedural rights, in order to enforce their rights. Third, the individual as a rights-holder may challenge state action which is contrary to the right to data protection.

Through the exercise of a number of data rights, the individual may operationalise data protection law by obliging the controller to treat their data in a certain fashion. One key data right is the right to access,[318] which has special place in the fundamental right to data protection, together with the right to rectification.[319] The CJEU has observed that the right to access one's data is necessary in order to facilitate the individual's other data rights.[320] Thus, once an individual has a copy of the data being processed in relation to them, the individual may be in a position to assess whether that processing is improper and seek to exercise other rights; to have inaccurate data rectified,[321] to have data erased,[322] to restrict processing,[323] to transmit that data to another controller,[324] or to object to certain processing activities.[325] These rights thus empower the individual to hold data controllers to account for the treatment of their data.[326]

If these procedural rights are not respected, or in some other way the individual's personal data is improperly processed, the individual is then armed with procedural rights to challenge this processing. The individual has a right to lodge a complaint with their local data protection authority.[327] The data protection authority is then required to handle that complaint and investigate, to the extent appropriate.[328] The individual may also mandate a representational entity to act on their behalf.[329] Should the individual be unhappy with the outcome of the investigation (or indeed any party subject to a legally binding decision of a data protection authority), they are entitled to an effective judicial remedy against the

[317] Article 7(4), GDPR.
[318] Article 15, GDPR.
[319] Article 8(2) of the Charter provides in part: "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
[320] C-553/07 *Rijkeboer* [2009] ECR I-03889, para 64; Joined cases C-141/12 and C-372/12 *YS and Others* (ECLI:EU:C:2014:2081), para 44.
[321] Article 16, GDPR.
[322] Article 17, GDPR.
[323] Article 18, GDPR.
[324] Article 20, GDPR.
[325] Article 21, GDPR.
[326] See further Ausloos (n 84).
[327] Article 77, GDPR.
[328] Article 57(f), GDPR.
[329] Article 80(1), GDPR.

authority.[330] The data subject also enjoys a right to an effective judicial remedy in respect of the infringement of their rights under the GDPR,[331] made potent by the guarantee that data subjects have a right to compensation for any material or non-material damage suffered.[332]

Armed with such procedural rights, it is often the individual who brings illegal processing to the notice of data protection authorities and the courts.[333] We can see plenty of evidence of this role in the many cases which have led to preliminary references to the CJEU which originate from individual complaints.[334] Of course, the individual is not the only agent to enforce data protection law; data protection authorities and representational entities may act without individual mandate.[335] Nevertheless, private enforcement of data protection law is an important component of the regime, particularly in light of the resourcing challenges of data protection authorities, which suggests that the capacity of data protection authorities to engage in systemic investigations beyond individual complaints is limited.[336] Thus the legal enforcement role of the individuals takes on even more practical significance.

Finally, alongside the specific procedural roles within the legislative scheme, the capacity of individuals to challenge state data processing activities in their status as a rights-holder, has been seen in multiple cases relating to Article 7 of the ECHR and Articles 7 and 8 of the Charter.[337] Notably, in the EU Courts, it is the individual who has the capacity to bring such challenges, whereas the CJEU has confirmed that an activist entity as a legal person had no standing to engage in such a challenge.[338]

Accordingly, while not the only agent of data protection law, the individual as a rights-holder and data subject plays an important role in enforcing data protection law, through the exercise of data rights, procedural rights and the fundamental right to data protection.

5. Questioning the multi-faceted role of the individual

The individual is central to the framing and operation of data protection law; we can see this through the examination of the multi-faceted role which the individual is playing, each aspect central to various aspects of data protection law: its objectives, its scope, its interpretation, its determination of legality and its enforcement. A clear understanding of how that concept is shaping data protection law is therefore a contribution to the understanding of data

---

[330] Article 78, GDPR.
[331] Article 79, GDPR.
[332] Article 82, GDPR.
[333] Advocate General Campos Sánchez-Bordona has characterised Article 82 as "part of a system of guarantees of the effectiveness of the rules in which private initiative supplements public enforcement of those rules." C-300/21 *Österreichische Post AG* Opinion of Advocate General Campos Sánchez-Bordona 6 October 2022 (ECLI:EU:C:2022:756), para 45.
[334] E.g C-131/12 *Google Spain and Google* (ECLI:EU:2014:317)*;* C-212/13 *Ryneš* (ECLI:EU:2014:2428); C-201/14 *Bara and Others* (ECLI:EU:C:2015:638)*;* C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650); C-582/14 *Breyer* (ECLI:EU:C:2016:779)*;* C-398/15 *Manni* (ECLI:EU:C:2017:197); C-73/16 *Puškár* (ECLI:EU:C:2017:725); C-434/16 *Nowak* (ECLI:EU:C:2017:994); C-498/16 *Schrems v Facebook Ireland Ltd* (ECLI:EU:C:2018:37).
[335] Articles 57 and 80(2), GDPR.
[336] 'Data Protection in the European Union: The Role of National Data Protection Authorities' (European Union Agency for Fundamental Rights 2010) <https://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf>. 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities' (European Data Protection Board 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> accessed 28 April 2019.
[337] See section 3.1 above.
[338] T-670/16 *Digital Rights Ireland v European Commission* (ECLI:EU:T:2017:838).

protection law itself. However, it is incomplete. Once we recognise that the individual is playing such a central role to the EU data protection regime, an evaluation of each aspect of their role and the multidimensional nature of the individual within the regime offers us a way in which to evaluate the regime. This section engages in such an evaluation, by assessing each of aspect of the role of the individual in turn.

First, I consider the limits of a law which takes individual protection as its object. Second, I consider whether protection on the basis of individual subjects is the only way to protecting such subjects. Third, I consider whether the capturing of individuals as regulated subjects will undermine the protection of data subjects. Finally, I ask what the responsibilisation of data subjects as agents in their own protection means for achieving data protection.

5.1. What does it mean to take individual protection as the normative foundation of EU data protection law?

In section 2, I presented the finding that the individual and their protection serves as the normative basis of EU data protection law. While other interests can be relevant and weighed within the scheme of legality created by the GDPR (such as a controller's interest, the rights of third parties, national and public interests), the individual's status as the object of protection has a decisive legal significance beyond other interests. This necessarily invites a question, what is the consequence of focussing EU data protection law upon individual protection? When there is criticism of individualist approaches to data protection and information privacy law, we might ask ourselves is framing a regime around the protection of individuals limiting the manner in which we think about the importance of data protection?

While it does not appear to be controversial amongst mainstream privacy and data protection scholars[339] to take as a starting point the protection of individuals, a number of scholars have pointed to this as too narrow. Usually, these scholars propose additive approaches, where groups or collectives, or certain societal interests should *also* be the object of data protection.[340]

In the context of EU data protection, at least, there is no urgent call to do away with an individually oriented regime entirely and to replace it with something different.[341] This is not surprising, first, as since the advent of modernity, when the individual became the organising unit of modern society, Western legal regimes have usually organised themselves around the action and protection of individuals.[342] The individualist tendencies of data protection are connected to its historical and institutional context,[343] and shifting to alternatives involves grappling with these historical and institutional legacies and interconnections. Moreover, we should recall the primary law basis for EU data protection legislation is connected to an

---

[339] By contrast, the communitarian critique begins from the opposite perspective. Amitai Etzioni, *Privacy in a Cyber Age: Policy and Practice* (Palgrave Macmillan 2015).

[340] For example Luciano Floridi, 'Open Data, Data Protection, and Group Privacy' (2014) 27 Philosophy & Technology 1; Kirsty Hughes, 'The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015); Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475; Lynskey, 'Delivering Data Protection' (n 249); Bieker (n 70).

[341] By contrast, Waldman has made a case that an individual rights approach to information privacy in the US will never work. Ari Ezra Waldman, 'Privacy's Rights Trap' (2022) 117 Northwestern University Law Review 88.

[342] H Patrick Glenn, 'A Civil Law Tradition: The Centrality of The Person', *Legal Traditions of the World: Sustainable diversity in Law* (5th edn, Oxford University Press 2014) <https://doi.org/10.1093/he/9780199669837.003.0005>.

[343] See Chapter 3.

individual's fundamental right.[344] Given that any changes to the EU Treaties would be very politically difficult, the connection between data protection legislation and the fundamental right to data protection are of continuing relevance. As shall be explored in Chapter 3, taking individual protection as the object of data protection can be seen in the historical context of the emergence of liberal human rights and the European Union's fundamental rights project.

EU data protection law has from its outset been connected with an individual's fundamental rights, first to respect for private life and later data protection.[345] The question arises: has the connection to individual protection constrained EU data protection law to the consideration of individual interests to the exclusion of common or public interests in data protection. A number of scholars have criticised individualised rights-based approaches to privacy, which raise analogous concerns.[346] Notably, Cohen has argued that privacy rights provide a tautologically individualistic frame of reference.[347] Separately, Regan has argued that framing privacy in individual terms means that it comes to be persistently outweighed by competing interests which are framed in common or public interests.[348] Bieker would say this is true also of data protection, that a dualistic approach is necessary, to take account of the structural piece of data protection.[349]

There is some resonance between these concerns and the approach taken by the CJEU to the right to data protection.[350] That said, the CJEU is not so narrow as to be singularly focussed on the particular individual litigant before it. By the nature of the challenges before it, the Court is often considering the value of the right to personal data in the abstract, particularly when the Court comes to point to the need for a "fair balance" between competing rights and interests. Rather than focussing on the impact upon the sole rights-holder litigant, the Court seems to have some appreciation for the importance of the right to the class of rights-holders as a whole, although still in their status as individuals. In *Digital Rights Ireland,* the Court seemed aware of the cumulative effect of surveillance on individuals,[351] and echoed in subsequent cases concerning bulk and indiscriminate surveillance.[352]

---

[344] See section 2.2(a) above.
[345] See Chapter 3.
[346] See Introduction, section 3.
[347] Julie E Cohen, 'The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy' (2018) 31 Philosophy & Technology 213, 226.
[348] Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (n 45).
[349] Bieker (n 70).
[350] One limitation in analysing these cases should be acknowledged. The majority of these decisions involve both Article 7 and Article 8 of the Charter. While I am focussed on the Article 8 approach, there are some challenges in parsing the reasoning of the CJEU, which tends to be brief and often conflated with the Article 7 analysis. This challenge, associated with the lack of case law which deals with data protection distinctly from respect for private life has also been noted by Bieker. ibid 7.
[351] The Court notes that the collection of communications data "taken as a whole, may allow very precise conclusions to be drawn", including concerning "social relationships" and "social environments." The Court further considers the cumulative nature of the interference with rights, noting that the Data Retention Directive "covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population." Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238), paras 27 and 56.
[352] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970); C-623/17 *Privacy International* (ECLI:EU:C:2020:790); C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791); Case C-140/20, *Commissioner of an Garda Síochána and Others* (ECLI:EU:C:2022:258).

However, while the Court often expressly notes that the right to data protection must be considered in relation to its function in society, this formulation is emphasised when the Court is considering the limits of the right, and its non-absolute nature.[353] A good example of this approach is seen in *Google France v CNIL,* wherein the CJEU considers the appropriate territorial scope of a de-referencing obligation upon Google.[354] If ordered to de-list a URL by the French authority – must Google de-list that URL only in the European Union or globally? The CJEU emphasised that the objective to provide a high level of protection of individuals and the impact of the access to the relevant information in the European Union could in principle justify a requirement for global de-referencing.[355] However, when the CJEU determines that a territorial limitation is appropriate, it then refers to fact that "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[356]

Thus, when the CJEU comes to specifically consider the relationship between data protection and society, the CJEU does not seem to acknowledge any particular importance of data protection on a collective or communal basis.[357] Rather, data protection is typically framed as an individual interest: something which might be detrimental to societal interests and therefore overridden in order to protect those societal interests.

When we remember that the GDPR sets out to protect not only the right to data protection, but multiple rights and freedoms,[358] this picture of the importance of data protection seems incomplete. Perhaps, an individual's fundamental right to data protection is intended to operate at an individual level, as a safeguard to the individual interest in their personal data. However, this should not speak to the entirety of the EU data protection project. If EU data protection law is to contribute to a data society in which fundamental rights and freedoms are at the core of our thinking, within a single market supported by a free movement of data, a purely individualist understanding of data protection is unduly narrow. The GDPR as a legislative project (and as the grounding for the wider EU data strategy) invokes a balancing of rights and freedoms of natural persons, there is a valuable opportunity to question our individualist lens and consider what we achieve together, both in how data protection is to serve us as individuals but also how it serves us collectively and societally. Implicitly, the right to data protection and the GDPR are already contributing to our societal picture of data protection, through its operation, and perhaps it is time to bring that debate out explicitly.

One source of inspiration for alternative conceptions of both the right to data protection and the balance between that right and other rights, freedoms and objectives may be the jurisprudence of the ECtHR. A number of academics have noted differences of scope

---

[353] See C-92/09 *Volker und Schecke and Eifert* [2010] I-11063*,* par 48; C-291/12 *Schwartz* (ECLI:EU:C:2013:670), para 33; Opinion 1/15 PNR (ECLI:EU:C:2016:656), para 136; C-136/17, *GC and Others* (ECLI:EU:C:2019:773), para 58, C-507/17 *Google France v CNIL* (ECLI:EU:C:2019:772), para 60; C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962), para 56; C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601), para 70.

[354] C-507/17 *Google France v CNIL* (ECLI:EU:C:2019:772).

[355] ibid paras 54-58.

[356] ibid, para 60.

[357] We can draw a contrast to the way the CJEU characterises freedom of expression, by way of simple example, which is imbued with democratic value in the Court's discourse. That right, also protected by the Charter is said to "constitut[e] one of the essential foundations of a pluralist, democratic society". Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970), para 93.

[358] Per Article 1(2), GDPR. "The Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." See Ausloos (n 84) 75–76.

between the two regimes, both in the broader material scope of data protection under the Charter as compared to under the ECHR and the enhanced data rights granted to data subjects by EU data protection legislation.[359] We might also consider the reverse relationship—what does the right under the ECHR offer or protect that has not yet been seen before the CJEU or in EU legislation? The conceptual development of data protection under Article 8 of the ECHR, as well as how private life has been extended to informational issues more broadly, are worth further exploration. The legal connection between the interpretation of Articles 7 and 8 of the Charter and Article 8 of the ECHR via Article 52(3) of the Charter has already been noted,[360] thus the necessary link to import reasoning from the ECHR is present.[361]

While this thesis is not founded on a complete systematic mapping of the jurisprudence of the ECtHR on data protection issues, from even some selected leading cases we can identify a starting point on considering alternative conceptions of data protection. Two particular observations are worth considering in terms of conceptions of rights before the ECtHR.

First, the ECtHR's decisions routinely engage with the need to strike a fair balance between various rights and interests, and there is a developed body of decisions regarding the conduct of such balancing exercises, including in relation to private life and data protection. Thus we frequently see the ECtHR emphasise the need to balance the individual's right with other competing rights and public interests. For example, in *ML and WW v Germany,* the ECtHR considers the need to strike a fair balance between the applicants' right to respect for private life, the radio station's and publishers' freedom of expression and the public's freedom of information.[362] The ECtHR has a developed jurisprudence on each of these rights and freedoms and thus is able to provide a series of principles to guide this balancing exercise.[363] A similar approach was seen in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* with regard to the relationship with freedom of expression.[364] Moreover, in some of the ECtHR's decisions, there is a sense of the holistic nature of the balancing to be struck between the various protected rights. The ECtHR has stated that in resolving the positive and negative dimensions of the various obligations under the ECHR, regard must be had to "the fair balance to be struck between competing interests of the individuals and the community as a whole.[365]

Second, the conception of the importance of data protection and informational privacy before the ECtHR is sometimes articulated beyond the individual. For example, in relation to cases

---

[359] Lee Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247; Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 522; Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; J Kokott and C Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.

[360] See section 2.2(a) above.

[361] Indeed, the CJEU sometimes explicitly draws upon ECtHR cases in data protection cases. See for example, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* [2003] ECR I-5014; C-92/09 *Volker und Markus Schecke and Eifert* [2010] I-11063; C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791).

[362] *ML and WW v Germany* App nos 60798/10 and 65599/10 (ECtHR, 28 June 2018), para 89.

[363] ibid, paras 96 – 115.

[364] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR, 27 June 2017).

[365] E.g. *Liebscher v Austria* App no 5434/17 (ECtHR, 6 March 2021), para 61.

concerning mass surveillance, a conception of collective harms associated with such surveillance is evident. In the context of a complaint regarding systems of secret surveillance, in *Szabó and Vissy v Hungary,* we see awareness of collective oppression associated with mass surveillance, as the ECtHR expresses concern "if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives."[366] Thus, we see consideration of the cumulative effect of individual rights' intrusion. Similarly, in *S and Marper v United Kingdom,* in considering the retention of cellular samples, DNA profiles and fingerprint data for law enforcement purposes, the ECtHR refers to "[t]he interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information."[367] Thus, this is another example of the ECtHR identifying a common interest in the protection of such data. Further, the ECtHR has also linked the individual interest in private life to broader public interests. In *Z v Finland,* the ECtHR noted that the protection of health data "is a vital principle in the legal systems of all the Contracting States…. not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general."[368] Moreover, the interconnected nature of private life has also informed the conception and application of Article 8 before the ECtHR.[369] In *Gaughran v United Kingdom,* the ECtHR considered the retention of DNA profiles.[370] The ECtHR took a relational approach to such data and the assessment of the legality of retention of such data, "because retaining genetic data after the death of the data subject continues to impact on individuals biologically related to the data subject."[371]

Thus, in beginning to think beyond the individual as the normative foundation of EU data protection law, as it has manifested in EU legislation and decisions of the CJEU to date, at least one source of inspiration may be the decisions of the ECtHR. Founded on a corresponding right to respect for private life, which encompasses data protection, there is a legal link to the Charter rights. Helpfully, we can see some broader conceptions of both the individual right (as balanced against other rights and interests) and of less individualistic approaches the importance of data protection.

5.2. Is the focus on individual subjects as protected subjects underinclusive or misdirected?

As a regime ordered around the protection of individual subjects, we might ask whether this is the most effective way to structure EU data protection law.

In particular, we might consider the way in which the scope of EU data protection law is tied to individual experience, and the resultant desire to protect personal data has led to an expansion of the scope of EU data protection law. Both the conception of identifiability and "relating to" the individual have been interpreted expansively.[372] The breadth of the concept of data protection has come under criticism. When, as Ohm has argued, almost any data

[366] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016), para 68.
[367] *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 104.
[368] *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997), para 95.
[369] See further, Chapter 4 section 3.1.
[370] *Gaughran v United Kingdom* App no. 45245/15 (ECtHR, 13 February 2020).
[371] ibid, para 81. See also *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 75.
[372] See section 3.2(b) above.

can be related to an underlying individual and anonymisation is near impossible,[373] it suggests that most data is personal data, and therefore most data is regulated by EU data protection law. Purtova has argued that the result of this broad conception of personal data, the evolving capacity of data analytics and the broader datafication of so many aspects of life will result in "circumstances where everything is personal data and everything triggers data protection", and the regime of rights and obligations under the GDPR will be "impossible to maintain in a meaningful way."[374] Dalla Corte has responded to these arguments with more optimism, arguing that there is space for a narrower and more nuanced vision of the conception of data protection.[375] He argues that this may be achieved through the proper interpretation of the "relating to" requirement in the definition of personal data.[376] In each case, Purtova and Dalla Corte seem to be arguing for a narrowing of the conception of personal data; either through regulatory reform or refined interpretation, but to maintain a focus on individually oriented approaches. Dalla Corte argues that data protection is an individual right, and meant to protect individuals rather than groups; and that the "relating to" link is critical to the conception of personal data.[377]

However, we might ask, do we always need to protect individuals through an individually-mediated approach? Both Purtova and Dalla Corte seem to be approaching the data subject protection on the assumption that it can only be achieved if we protect the natural person *qua individual.* This has an inevitable scaling effect: cases need to be dealt with on an individual-by-individual basis, and in circumstances where datafication is so prevalent, this is always going to be challenging for regulators to oversee. We see this in the manner in which personal data is defined in terms of the individual and legality is adjudged by reference to individual data subjects in many provisions of the GDPR.[378] It is possible to think beyond this framing, even where we take the individual as the object of protection. For example, Cohen and Lynskey have pointed to the need to focus on the material and social conditions to which individuals are subject in order to better achieve data privacy and data protection.[379] We can accept that data ought to be protected due to the impact it may have on individuals and nevertheless choose to approach the protection of those individuals through the reform of structural or environmental practices.

Indeed, there are hints to the possibility of such an approach already within the existing data protection framework. If we consider both the apparent assumption of the legislature and CJEU that a broader remit of protection is better protection, and Purtova and Dalla Corte's theories that narrower approaches are the only response to the impracticalities of broad protection, it is worth examining the hybrid concept of "special categories of data", also known as "sensitive personal data".[380] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or processing of genetic

---

[373] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.
[374] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86) 75.
[375] Dalla Corte (n 86).
[376] ibid.
[377] ibid 10.
[378] See section 3.2.
[379] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1; Lynskey, 'Delivering Data Protection' (n 249).
[380] Article 9, GDPR. The protection of genetic and biometric data have been added to the category as additions to the protections of the Data Protection Directive. Additionally, data relating to criminal activity has been separated from Article 9, GDPR, and subject to a separate regime in line with the introduction of the Law Enforcement Directive.

data, biometric data, health data or data concerning sex life or sexual orientation attract special and additional protection. This makes an interesting counter-perspective to Purtova and Corte for a couple of reasons. First, I name it a "hybrid" concept, because while it is unquestionably aiming to protect individuals, it does so by reference to group characteristics, in an apparent recognition that certain groups may suffer disproportionately through the abuse of their personal data.[381] Second, it demonstrates that the regime may be broad, but also offers a depth of protection to more egregious harms. Arguably, it demonstrates a recognition of particularly harmful forms of data processing–those which target certain protected characteristics—and the imposition of additional protective safeguards on processing of such data. This aligns with Purtova's suggestion that a focus on data processing outcomes, and in particular safeguarding against "information-induced harms" might be a more workable and protective regulatory regime.[382]

Without advocating for such an approach to be adopted nor disregarding the institutional and administrative challenges of a broad regime, nevertheless, it does show a degree of flexibility already inherent in the regime to address particularly harmful practices, as well as an alternative vision for the protection of individuals.

In order to extend this analysis of what a framework not ordered by individual subjects might look like, we might also ask, what does the current framework based on individuals omit? By limiting the regime to concerns of the individual, we do not think about groups who might need to be protected by virtue of group characteristics, or questions as to the type of digital environment which benefits society as a whole. By framing the regime around individuals in isolation, without regard to the groups and collectives to which they might belong, or as embedded citizens in a society and democracy, EU data protection law has adopted a particularly individualistic understanding of the person.

5.3. Will the designation of individuals as regulated subjects achieve greater protection of data subjects?

The expansion of the concept of a data controller and joint controllership, and the parallel narrowing of the household exemption has resulted in a legal situation where a growing number of individuals may be regarded as subject to the obligations of the GDPR as regulated data controllers.[383]

The possibility of individuals to be regulated as data controllers has traditionally received limited attention. For example, Van Alsenoy, in his book on the relative roles and responsibilities of controllers and processors, only considers the capacity for individuals within organisations to be considered controllers,[384] but does not consider the capacity of an independent individual to be a controller. Elsewhere, he has criticised the possibility demonstrated in the *Lindqvist* and *Rynes* case of the application of data protection law to the activities of such individuals acting in a predominantly private capacity.[385] But there is a growing awareness and criticism of the emergence of this phenomenon through the CJEU's decision making on joint controllers. Edwards et al have criticised this "'everyone is a controller'" approach, [386] as have Finck and Mahieu et al.[387]

---

[381] On the differential impact of surveillance and processing, see further Chapter 6.
[382] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86) 79–80.
[383] Described in section 3.4 above.
[384] Van Alsenoy (n 302) 117–121.
[385] Van Alsenoy (n 83) 6.
[386] Edwards and others (n 83).

It seems we might do well to heed the warnings of Advocate General Bobek, who advised us:

> *"Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted."*[388]

The legal determination that an entity is a data controller does not necessarily result in better data protection law. First, any equivalence between well-resourced and revenue generating organisations and the user of a platform who has some decision making over particular features in the context of the joint-controller cases seems misplaced. The concept of controllership, and all the associated obligations, and procedural mechanisms created, is premised on an institutional understanding of the controller.[389] If, as some have argued,[390] one of the purposes of data protection is to counter balance the asymmetries of power between powerful data controllers and individuals, this false equivalence would seem to undermine this purpose. Not all controllers are the same. In the language of Laidlaw, some platforms may be considered "gatekeepers" in the sense that they can control access to information, or can go further and impact democracy through their shaping of the environment in which speech is shared.[391] While Laidlaw was concerned with freedom of expression issues, her concern about the greater responsibilities which might be attached to certain powerful actors is similar to the approaches adopted in the Digital Markets Act and Digital Services Act.[392] The measure of influence that an individual data controller may have on the nature of data processing conducted on the platform or infrastructure operated by a large organisational data controller may be sufficient from the perspective of the CJEU's ruling to render them a legally responsible data controller, but in doing so, there would seem to be considerable risk of creating significant enforcement challenges.

Effective data protection is contingent on practical considerations, including administrability and enforcement capacity. This can be challenging enough for commercial entities. The capability of individuals to comply with the onerous regime, the possibility that individuals would even be aware of their legal responsibilities and the potential for commercial operators to shift responsibility to their customers would seem to make this "complete and effective protection" that the CJEU is purporting to ensure entirely illusory.

---

[387] Rene Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World – On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 39; Finck (n 83).

[388] C-40/17 *Fashion ID* Opinion of Advocate General Bobek 19 December 2018 (ECLI:EU:C:2018:1039) para 82.

[389] Discussed in section 3.4 above.

[390] Lynskey, *The Foundations of EU Data Protection Law* (n 86); Bieker (n 70).

[391] Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24 International Review of Law, Computers & Technology 263.

[392] REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12102022, p 1–66); REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277/1, 27102022, p 1-102).

5.4. Is it appropriate to expect individuals to defend their own interests as agents of data protection law?

The role of individuals as agents of data protection may be questioned, when we consider the capacity to engage in self-defence is limited by the digital environment in which individuals operate, personal circumstances and capacity, and the resources at their disposal (both personal and in the form of public support).

The challenges associated with decision making in the digital environment is well recognised, and they have seemingly informed the addition of limitations to the concept of consent under the GDPR.[393] For a variety of reasons, individual decision making in a datafied environment is challenging and may not result in protective outcomes. The challenges which individuals face in each instance of decision making are compounded by issues of scale.[394] As Mai points out, there has been a massive expansion of the amounts of information which is being produced and processed.[395] Consequently, the number of decisions which individuals are presented with have expanded beyond which anyone could meaningfully address. For, Hartzog, this is a fatal flaw—the concept of control cannot meaningfully scale and therefore "will never work for personal data mediated by technology."[396]

However, the question of individual responsibility and responsibilisation,[397] beyond the legalisation of processing through consent or contractual necessity, has received little attention.[398] We have seen that the individual, as an agent of data protection, is equipped with a range of data rights and procedural rights, so that they might defend their own interests. Matzner et al. question the reliance on such "do-it-yourself data protection" premise.[399] While they focus on technological approaches to safeguarding one's own privacy (such as cryptography and anonymisation tools), their conclusions as to the non-viability of such approaches may also be applied to legal responsibilisation through the grant of remedies to be individually exercised. As they recognise, "[b]eing aware of and understanding the technical architecture behind online information flows becomes harder and more complex with the rapid growth of new technologies."[400] As a result, they caution

---

[393] See further Chapter 5.

[394] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 35) 1888. Lynskey, *The Foundations of EU Data Protection Law* (n 45) 247.

[395] Mai (n 30) 196.

[396] Hartzog (n 310) 426.

[397] Responsibilisation is generally situated in criticism of neoliberalism, and in particular a vision of a shrinking state mandate in favour of *inter alia* "increased emphasis on personal choice and freedom." Susanna Trnka and Catherine Trundle, 'Competing Responsibilities: Moving Beyond Neoliberal Responsibilisation' (2014) 24 Anthropological Forum 136, 137.

Merry has argued that rights-based approaches are based on a particular vision of a responsibilised subject, "who makes his or her self through choices rather than through relationships" and that responsibilisation "emphasises rational choice and self-interest defined in economistic terms of costs and benefits." Sally Engle Merry, 'Relating to the Subjects of Human Rights: The Culture of Agency in Human Rights Discourse' in Michael Freeman and David Napier (eds), *Law and Anthropology* (Oxford University Press 2009) 403.

[398] The responsibilisation of the subjects of data protection law is not unique in EU law, (*see* Damian Chalmers, 'The Unconfined Power of European Union Law' (2016) 1 European Papers 405.) but nevertheless seems to be underexplored.

[399] Matzner and others (n 310).

[400] ibid 287.

that “the danger arises that data protection regulations shield a space for autonomous decisions that … are impossible to carry out.”[401]

The data rights and procedural rights granted to the individual purport to enable them to protect themselves. Yet, this approach has the same flaw that a consent-based approach does, as we suffer from what Hartzog names a “bandwidth problem”: “People only have twenty four hours in a day and every company wants you to make choices.”[402] This catalogue of rights presumes both that an individual has the capacity to monitor the data processing to which they are subject, much of which is opaque, and will know that they do have such rights and how to exercise them. For this reason, Blume has argued that “data protection law appears more citizen-friendly than it actually is.”[403]

Alongside the question of individual capacity to exercise such responsibility, we must also ask whether individuals should be required to exercise such responsibility. Matzner et al reject individual responsibility, and argue for data protection as a social responsibility.[404] Matzner et al identify that locating data protection primarily with the individual has a series of implications; including framing lack of data protection as a choice, transforming the protected individuals into consumers and creating a gap whereby social inequalities concerning data protection cannot be adequately addressed.[405] Cohen has argued that in this fashion privacy laws may legitimate a power structure in which data harvesting commercial enterprises are insulated from accountability.[406]

The question of whether individuals can or should exercise control or manage their own data in this fashion will be returned to in later chapters,[407] nevertheless, at this venture we can make some preliminary observations. The question of the individual’s role in this regard is broader than one of control, and conceiving of the individual as an agent of data protection opens up the issue of the enforcement model of EU data protection law, including the balance between public and private enforcement, and the risks associated with deputising individuals with the defence of their own interest when they are not equipped with the means to meaningfully do so, or in an environment where such defence is often not practically possible.

6. A reflection on this framework of the individual: examining the individualism of EU data protection law

This chapter has offered an account of the legal role of the individual within EU data protection law, and having set out the individual’s position as the normative anchor, central subject and agent of data protection law, and in doing so, makes a case for the centrality of the individual to the overall legal regime. However, this is not a complete account of the EU data protection regime, and I do not contend that the regime is only concerned with the individual’s role or interest. Rather, we can point to countervailing aspects of the regime which are not framed in terms of the individual natural person, which illustrate that the regime cannot be said to be entirely individualistic. In a mirror to the framework offered, I offer some thoughts on the ways in which non-individualist normative interests, subjects and agents also inform the interpretation and application of EU data protection law.

---

[401] ibid 296.
[402] Hartzog (n 310) 429.
[403] Blume (n 59) 260.
[404] Matzner and others (n 310) 294.
[405] ibid 296.
[406] Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27).
[407] See further Chapter 5.

6.1. Non-individualist normative considerations

Normative concerns beyond individual protection are present in the EU data protection regime. Notably, within the GDPR itself, we also see interests beyond the individual attain legislative protection, either as express objectives to be served, or interests and rights to which the individual's right to data protection might give way.

First, the economic or market making objective of data protection, while less central than under the Data Protection Directive,[408] still finds significance within data protection. Free movement of data is still an objective of the GDPR.[409] The GDPR, in setting a (mostly) harmonised set of data protection standards seeks to facilitate the exchange of data across Member State borders.[410] This is conceived as partially an economic project, as the GDPR contends that

> *[t]he proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*.[411]

Thus, we see many places in which the economic nature of the data protection project is incorporated into the GDPR.[412] This is evident, for example, in the recognition that the activities pursued by data controllers may be a legitimate interest which provides a lawful processing of personal data, which can be associated with service provision,[413] or indeed the broader notion of data being processed in association with the provision of goods or services,[414] though the notion of data as consideration or counter-performance goes beyond the conceptions found in the legislation.[415] Moreover, as described above in section 2.2(b),

---

[408] See section 2 above.
[409] Article 1(3), GDPR.
[410] Recitals 5 – 13, GDPR.
[411] Recital 13, GDPR.
[412] These economic ties have led to a body of literature on the potential roles for competition law and consumer protection law in regulating data protection issues. For example, see C Kuner and others, 'When Two Worlds Collide: The Interface between Competition Law and Data Protection' (2014) 4 International Data Privacy Law 247; Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (Oxford University Press 2016); Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11; Natali Helberger, Frederik J 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; Damian Clifford, 'Data Protection and Consumer Protection: The Empowerment of the Citizen Consumer' in Gloria González Fuster, Rosamunde E Van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022) 229.
[413] Within the balancing test envisaged. See Article 6(1)(f), Recital 47 and 48, GDPR.
[414] For example, Article 3(2)(a), Article 4(15), Article 7(4), Article 8, Article 27(3), Article 28(3)(g), GDPR. See also the references of the CJEU to economic connections between establishments in clarifying the geographical reach of data protection law. In *Google Spain,* the CJEU finds that "*the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed*." C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 56. This approach has been subsequently followed in a number of cases concerning establishment. See C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388), para 60; C-507/17 *Google France v CNIL* (ECLI:EU:C:2019:772), para 50; C-645/19 *Facebook Ireland and Others* (ECLI:EU:C:2021:483), para 94.
[415] Clifford (n 412).

at least in regards to the influence in the Court's purposive interpretation of the legislative framework, this economic or market making objective is rarely given such legal prominence as the GDPR's protective aims.

Other normative interests also come to be incorporated through the accommodation of many countervailing parties, rights, interests and principles to be weighed against the individual's data protection interest. These might be said to be principles and interests which permissibly undermine or interfere with the individual interest in data protection, given the non-absolute nature of the right to data protection. Within the legislative scheme of the GDPR, we see express recognition that an individual's data interest may be accommodated to facilitate interests such as public interests in data processing, [416] the defence of legal actions,[417] the use of data for certain archiving and research purposes,[418] and the protection of freedom of expression and information.[419]

The right to data protection itself can be limited when balanced against other rights and objectives. In the Charter, Article 52 allows the interference with the individual's right to data protection in prescribed circumstances. Such permissible limitations may be made *inter alia* "if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[420] In this sense, the right to data protection comes to be balanced against competing rights and freedoms of other persons (e.g. the right of freedom of expression,[421] general objectives such as public security and the fight against serious crime).[422] As has been discussed previously, in these cases, the CJEU tends to emphasise the individual nature of data protection in the balancing exercise,[423] and there is some echoing of early criticisms of Regan, that individualistic framings of privacy come to be seen as less significant when weighed against interests framed as common or public goods.[424]

6.2. Other key legal subjects

In section 3 above, the individual has been presented as a central legal subject within EU data protection law, by virtue of their status as a rights-holder, data subject, other protected natural person and at times, a data controller. Of course, there are other legal subjects created or recognised by EU data protection law. The data controller and data processor are invested with legal status as the responsible and accountable entities under the GDPR, and in doing so the legislative scheme attaches obligations and duties to the entities which

---

[416] Recital 45, 46, Article 6(1)(e), Article 9(2)(g). See further Article 86, 87 GDPR, and the manner in which Member States can further derogate using national legislation under Article 23, GDPR.
[417] Articles 9(1)(f), 17(3)(e), 18(1)(c), 21(1), 49(1)(e), GDPR.
[418] Article 5(1)(b), Article 5(1)(e), Article 9(2)(j), Article 14(5)(b), Article 17(3)(d), Article 89, GDPR.
[419] Recital 4, Recital 153, Article 17(3)(a), Article 85, GDPR.
[420] Article 52(1), GDPR.
[421] See e.g. C-131/12 *Google Spain and Google* (ECLI:EU:2014:317); C-136/17 *GC and Others* (ECLI:EU:C:2019:773); C-507/17 *Google France v CNIL* (ECLI:EU:C:2019:772); Case C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962).
[422] See e.g. C-291/12 *Schwartz* (ECLI:EU:C:2013:670); Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238); Joined cases C-446/12 to C-449/12 *Willems and Others* (ECLI:EU:C:2015:238); Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656); Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970; C-673/17 *Planet49* (ECLI:EU:C:2019:801); C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791).
[423] See section 5.1 above.
[424] Regan (n 45).

determine “the purposes and means of the processing of personal data”, or are so nominated under legislation, and persons who process data on their behalf.[425]

Accordingly, the controller, and the data processor to a lesser extent,[426] also have legal significance as subjects of the EU data protection regime.[427] The nature of the obligations and duties of the data controller have already been introduced above in the context of their mis-fit with the classification of individuals as controllers.[428] As the target of regulation, the controller does shape some of the logic of the regime. The territorial scope of the GDPR is defined in terms of either the controller’s place of establishment or the nature of their activities (in connection with the location of the affected data subjects.)[429] The legal bases of compliance with a legal obligation and necessity for the purposes of legitimate interests of a controller both place the controller centrally.[430] The data protection principles target the controller’s approach to data holistically,[431] and a number of scholars have pointed to the data protection principles in particular as a potential area for less individualist approaches to data protection.[432] Substantive obligations are created which are described in terms of the controller, as it is for them to address them.[433] We have seen the CJEU articulate the controller’s compliance duty in terms of the particular controller, in the context of the right to be forgotten cases, requiring that

> *the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 and of the GDPR in order that the guarantees laid down by that directive and that regulation may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.*[434]

If we consider the obligation of data protection by design, and the security obligation, these obligations in particular are shaped by the activities of the controller, as the protective measures to be taken should take into account *inter alia* “the cost of implementation and the nature, scope, context and purposes of processes,” alongside the impact upon affected natural persons.[435] In addition to the general principle of accountability,[436] many of the provisions of the GDPR place an express burden of compliance on the controller, such as the requirement to demonstrate consent,[437] certain age-verification steps,[438] and identity verification more broadly,[439] the designation of representatives,[440] record-keeping,[441] security

---

[425] Articles 4(7) and 4(8), GDPR.
[426] See Article 28, GDPR.
[427] For a good problematisation of this division of responsibility, see Van Alsenoy (n 302).
[428] See section 3.4 above.
[429] Article 3, GDPR.
[430] Article 6(1)(c) and (f), GDPR.
[431] Article 5, GDPR.
[432] van der Sloot, ‘Do Data Protection Rules Protect the Individual and Should They?’ (n 60); Damian Clifford and Jef Ausloos, ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130; Lynskey, ‘Delivering Data Protection’ (n 249) 83; Bieker (n 70).
[433] On transparency, see Article 12, GDPR; on compliance with data subject rights, see Articles 13-22, GDPR; on data protection by design and design, see Article 25, GDPR; on data transfers to third countries, see Article 44-49, GDPR.
[434] C-460/20 *TU, RE v Google LLC* (ECLI:EU:C:2022:962), para 51. (My emphasis.)
[435] Article 25(1), GDPR; Article 32, GDPR.
[436] Article 5(2), and Article 24, GDPR.
[437] Article 7, GDPR.
[438] Article 8(2), GDPR.
[439] Article 11, GDPR.

breach notifications,[442] conducting impact assessments in certain cases,[443] consulting with DPAs,[444] and appointing a data protection officer in some cases.[445] In the emergence of the notion of the controller's "responsibilities, powers and capabilities", these obligations are being interpreted by the CJEU by reference to particular controller circumstances,[446] thus demonstrating that the controller as legal subject also has an important role in the EU data protection regime.

In this sense, there is an aspect of EU data protection law which is non-individualist in a supportive sense, in the creation of structural forms of data protection – scaffolding of rules and principles which govern data protection, even without reference to the individual data subject, which might be said to create a more "data protection friendly" environment, from which the individual benefits incidentally.[447] These rules which target the controller's activities, may be said to create a baseline of responsible or reasonable processing.[448] In this sense, EU data protection law has a structural dimension.

Thus, when we consider the regulated subjects of EU data protection law beyond the individual, the data controller's role and status is certainly important to the regime; guiding the territorial threshold of application, and being the subject of the core obligations of the GDPR. Nevertheless, neither the controller nor processer can be said to shape the logic of the regime to as great an extent as the individual which shapes the material scope of the regime, is central to the assessment of the legality of processing, and most significantly grounds the normative basis for and legitimacy of the regime.

6.3. Other agents of EU data protection law

I have characterised the individual as an agent of EU data protection law, in their role as a decision-maker over the use of their personal data, and in their recourse to the procedural protections of EU data protection law. They are not the only agents of data protection law, of course. Data controllers, data protection authorities, the courts, and representative bodies, in particular, also have important legal functions in the completion of EU data protection law. The role of the data controllers in satisfying the requirements of data protection law and the compliance measures which are created by the GDPR have been described in the foregoing

---

[440] Article 27, GDPR.
[441] Article 30, GDPR.
[442] Article 33-34, GDPR.
[443] Article 35, GDPR.
[444] Article 36, GDPR.
[445] Article 37-39, GDPR.
[446] The CJEU has held that the operator of the search engine was responsible to ensure its activity complied with the Data Protection Directive "within the framework of its responsibilities, powers and capabilities". C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 38. Subsequently, this has led to a specific interpretation of the obligations of search engine operators by reference to the particular service operated. See C-136/17 *GC and Others* (ECLI:EU:C:2019:773), paras 44-48; C-460/20 *TU, RE v Google LLC* (ECLI:EU:C:2022:962).
[447] Bieker suggests this understanding of structural data protection, grounded in key principles which he derives from the legislative scheme: lawfulness, purpose limitation, necessity and data minimisation, storage limitation, separation, confidentiality, integrity and availability, transparency, control and accountability. Bieker (n 70) ch 5.
[448] Van der Sloot points to the origins of these principles in the 1970s and argues "the focus of these principles was on the fairness and reasonableness of the data processing, for example by specifying that data should not be collected and processed when this was not necessary for or proportionate to the goal pursued and by laying down that the data should be correct and kept up to date, so as to guarantee that the profile of a person or a group of people was accurate." van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60).

section, so I will consider in further detail the significance of the DPAs', courts' and representative bodies' roles in the operation of EU data protection law.

The primary role which data protection authorities and the courts play in EU data protection law is as public enforcers of the law. Data protection authorities are charged with "monitoring the application of [the GDPR], in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[449] Public enforcement of data protection by an independent authority is protected within the right to data protection in Article 8(3) of the Charter, and the importance of that independence has been reinforced in the GDPR,[450] and in a number of decisions by the CJEU.[451] In order to monitor the application of the GDPR, DPAs are empowered with a series of powers within their Member State,[452] and assigned a wide series of tasks–including monitoring and enforcement, promoting awareness and advising national institutions, handling complaints and conducting investigations.[453] These tasks are very broadly drafted, and we can see on the terms of the GDPR, the DPAs' roles in achieving data protection from advisory, awareness and enforcement perspectives is considerable. It will of course still be connected to an individual interest, given the predominance of the individual role in the understanding of the importance of data protection and the significance of the data subject and other natural persons to the application and assessment of the legality of data protection.[454]

The courts, at both a national and EU level, also have an important role to play in the enforcement and operation of data protection law. As described in the context of the individual's procedural protections, the individual's capacity to challenge the decision of a DPA, or seek a judicial remedy against a processor or controller is contingent on the existence and effectiveness of the court system which hears such a challenge or claim.[455]

Finally, not-for-profit representative bodies are also invested with new enforcement roles in the GDPR, providing that they might represent data subjects' interests (either with mandate or without) by making a complaint to a DPA on the behalf of or in the interest of data subjects.[456]

On a concluding note, a more balanced vision of the multiple agents who contribute to the achievement of data protection law, the individual, the controller, the DPAs, representative bodies and the courts demonstrates both the centrality of the individual and their interest to the achievement of data protection law, but also the buttressing institutional protections which have been implemented to safeguard the individual by way of controller compliance and public enforcement. Such public oversight speaks somewhat to those who have criticised individualist privacy approaches. For example, Smuha advocates for a societal approach to AI, which she contrasts to an individualistic or collective approach, and points to the strategies of environmental law for inspiration.[457] In particular, she raises public oversight, public monitoring, procedural routes without individual harm locus standi

---

[449] Article 51, GDPR.
[450] Articles 52 and 53, GDPR.
[451] C-518/07 *Commission v Germany* [2010] ECR I-01885; C-614/10 *Commission v Austria* (ECLI:EU:2012:631); C-288/12 *Commission v Hungary* (ECLI:EU:C:2014:237).
[452] Article 55, GDPR.
[453] The full list of tasks is contained in Article 57, GDPR.
[454] See sections 2 and 3 above.
[455] Articles 78, 79, GDPR.
[456] Article 80(1) and (2), GDPR.
[457] Smuha (n 57).

requirements.[458] These suggestions bear some resemblance to the GDPR's enforcement through data protection authorities, though the GDPR does not go so far as to allow pure public interest cases, nor measures of harm which are disconnected from the individual, but nevertheless demonstrates that the EU data protection law regime cannot be said to be a strictly individualist approach.

7. Concluding – the multi-faceted role of the individual

This chapter has presented a framework for understanding the ways in which the individual is central to the framing and operation of data protection law. This centrality is seen through the examination of the multi-faceted role which the individual is playing, each facet central to various aspects of data protection law; its objectives, its scope, its interpretation, its determination of legality and its enforcement. In each of these areas of the law, the individual's interest and actions are prominent. Nevertheless, we cannot say the individual's role is entirely determinative in an absolutist individualist sense, as other important legal subjects and normative interests are accommodated within the regime, albeit to a lesser significance.

Individual protection serves as the objective for the operation of EU data protection law, a source of its legitimacy as well as the driving force in its interpretation and operation. The individual shapes the subject matter of regulation, as their interests shape the scope of the data protection law and is central to the assessment of legality under the GDPR. The individual is also critical to the operation of data protection, as they challenge data controllers and protect their own interests.

I suggest that a clearer understanding of how the role and place of the individual within the regime is shaping data protection law offers a contribution to the understanding of data protection law. First, it is important to recognise that the individual is playing several important parts within the regime, a matter which is often implicit rather than express in both the case law and scholarship. Moreover, by offering a framework for understanding the multiple ways in which the individual is relevant to the regime, an evaluation of each of these parts and the multi-faceted nature of the individual within the regime offers us more precise and nuanced parameters for analysis.

Recognising that the individual serves as the normative foundation of the GDPR, we can consider the consequences of this role. One might accept that the objective of protecting individuals is rooted in the EU primary law, through the fundamental right to data protection and yet be concerned that such an approach on current terms is insufficient to achieve data protection in a broader sense, that such a framing may at times be too narrow and can be underinclusive of societal interests in responsible data processing. We can see the inclusion of non-individualist normative concerns (such as free movement of data or the interest in research) as points of contrast, both demonstrating the fact that the individualist interest will not always prevail over other rights and interest, but also that there is no comprehensive vision of a societal approach to data protection. In subsequent chapters, the conceptualisation of the individual basis for data protection will be further interrogated.

Subsequently, even if we aim for individual protection, recognising that the EU data protection regime has adopted an approach based on protecting persons as *individuals*, rather than in other approaches, we can ask, do we always need to protect data subjects through an individually-mediated approach? Such an approach seems to have had a scaling effect in EU data protection law, which can contribute to enforcement and individual fatigue

[458] ibid 15–17.

challenges. This suggests the need to re-open the question of regulatory design in this field, and we can look to existing approaches (e.g. a higher threshold of scrutiny or protection in areas of higher potential harm, such as in the case of the processing of special categories of data) as inspiration for alternatives.

Moreover, once we recognise that individuals are acting as agents in their own self-defence, we might question whether it is appropriate to expect individuals to safeguard their own interests. The recognition of the challenges in terms of individual capacity, and the potential to recognise a social responsibility for data protection enforcement can allow us to re-examine the balance between public and private enforcement of data protection.

Further, the potential for individuals to be captured as the regulated entity of data protection, as a data controller or co-controller, due to the expanding interpretation of that concept and the narrowing of the household and purely personal processing exemption raises concerns. This designation brings into tension the inherent assumptions about the nature of controllers, and the resources they can bring to bear in achieving data protection compliance, and a potential mismatch with some business models or prevalent practices.

Moving beyond the critiques of these aspects in isolation, it is worth considering the individual holistically: what are the implications of the individual's multi-faceted role within EU data protection law? When we consider the intersecting nature of these facets, and in recognising that the regime also has non-individualistic dimensions, we are offered a means of assessing the regime and also possibilities for imagining alternative approaches. We can ask: does a desire to protect individuals necessarily invoke legislation premised on an individual subject, or individually exercisable rights? This, I suggest, is not inevitable, but a product of particular historical and institutional features, to be explored in the following chapter.

Finally, the picture of the individual and the challenges associated with their role which have been presented suggests that the limits of the role of the individual go to the heart of the challenges with the GDPR: its seeming lack of capacity to tackle systemic data abuses despite an ever-expanding scope, the mismatch between legislative designations and the digital environment, and the helplessness that individuals may feel as to the ability to control their data or defend their interests against data controllers.

CHAPTER 3: SHIFTING IDEAS OF THE INDIVIDUAL

The previous chapter has made the case that the individual holds a central place in EU data protection law, through its important multi-faceted role in the regime. This chapter seeks to further this discussion by asking – why is the individual central to the GDPR and the EU's data protection project?

This contribution argues that we should understand the centrality of the individual in association with the historical, institutional and cultural context of the law. While this chapter does not purport to offer a comprehensive history of EU data protection, rather it identifies two prominent factors which have shaped the place of the individual in EU data protection law. The first is the historical and conceptual connection of data protection to rights to privacy/respect for private life, and the emergence of European rights frameworks. The second is the European Union context itself, its economic order and its growing fundamental rights mission.

Once recognised, these contextual factors allow us to understand the notion of the individual which has taken shape in EU data protection law. The individual who emerges from these disparate sources is unsurprisingly not an entirely coherent or unitary construction, but rather conflicting ideas of personhood are evident. One such fragmentation is explored, as I argue that the individual as seen as both a citizen rights-holder within the regime, and also as a consumer and economic object.

1. Contextualising the role of the individual in EU data protection

This chapter does not seek to offer a comprehensive history of information privacy or data protection, nor of every conception of the individual which has been represented in European privacy laws. Rather, the claim is more limited, that we should understand the role of the individual in the context of the development of EU data protection law, and offers two relevant aspects of that development. To be clear, the claim is not that there has been a linear development of EU data protection law or norms from a fixed period of time to today, nor that these are the only relevant historical developments or contexts from which to understand EU data protection law. What I do contend is that two particular contextual developments inform EU data protection law. In particular, we can further understand the role and conception of the individual in EU data protection law by reference to: (i) the emergence of fundamental rights to privacy or respect for private life, and (ii) the creation and development of the European Union, its mission and legal order. A second observation which emerges from engaging with these developments is that ideas of privacy, private life and data protection are varied, and that appropriate legal protection of such concepts is not a matter of consensus. Accordingly, we are reminded that conceptions of the individual and the protection of their privacy or data protection are not uniform, and rather differences can be representative of contested ideological positions.

By way of methodological note, the account in this chapter seeks to link two particular historical developments with the place and understanding of the individual in EU data protection law. The account of these developments is acknowledged not to be a comprehensive history of all privacy laws and protections, nor narratives thereof, in Europe. Rather, it has been constructed by identifying landmark legal protections which were significant for the era, in either introducing a new form of protection in their respective jurisdictions or for representing particular ideas of privacy or private life. Thus, early notable

landmark constitutional protections of privacy in the Member States of the European Union (or their predecessor states) are noted.[459] These protections varied in their formulations, some concerned with "privacy", others with "private life", "secrecy" or "confidentiality". I adopt the nomenclature of "privacy" rights as an umbrella term to refer to such protections and rights collectively, but acknowledge this is somewhat reductive. Additionally, while all current privacy rights found in the text of the constitutions of Members States of the European Union are noted, this does not account for the developments of constitutional law which are found in domestic decisions or case law. With regards to protections which emerged from legislative or judicial developments, the examples cited are more limited. This is in part due to the limited availability of relevant materials in the English language, and thus where such cases or accounts are relied upon, they are intended to be illustrative of particular instances and not representing the position across Europe nor a comprehensive survey of all approaches across Europe. Similarly, where supranational legal protections of privacy, private life or data protection are noted, landmark developments have been noted. The legislative history of EU instruments has been considered only in brief, in relation to the inclusion of notion of privacy in the Data Protection Directive and GDPR.[460] Academic and relevant commentary on these developments has also been relied upon to situate such legal protections in their conceptual or ideological context.

The limitations of these methods should therefore be acknowledged. As this chapter is not founded on a comprehensive account of all forms of privacy protections which have emerged across Europe, it does not purport to offer such an account. Rather, the description of such developments as are noted in this chapter should be regarded in a more limited fashion. Commonalities across certain jurisdictions and approaches are seen, and conceptual links between political and academic writings and exemplar legal protections are observed. Thus, the argument is made that context is relevant to understanding contemporary EU data protection law and the role of the individual in that law, by illustrating *some* of that context and connecting it to current debates and legal approaches to data protection. Nevertheless, this is not an exhaustive account of all relevant context, historical or institutional, and therefore other aspects relevant to the role and conception of the individual in EU data protection law may be omitted.

2. Privacy and data protection

The notion of privacy is contentious and unsettled. The ambiguity of its meaning has inspired many conceptualisations and taxonomies.[461] Legally, it has expansive scope, protecting a wide range of interests (from one's sexuality and reproductive rights to protection against police surveillance). The history of privacy is also an important antecedent to the history of data protection, and its conception and legal protection has considerable influence on and overlap with the EU data protection project.[462] By examining the emergence of privacy as an

---

[459] Where possible, primary sources were relied upon, but in certain instances where English language versions were unavailable of the relevant constitutional documents, secondary sources were relied upon.

[460] See section 3 below.

[461] E.g. Ferdinand David Schoeman, 'The Meaning and Scope of Privacy', *Privacy and Social Freedom* (Cambridge University Press 1992); Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087; Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008); Adam Moore, 'Defining Privacy' (2008) 39 Journal of Social Philosophy 411; Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

[462] David Erdos, 'Comparing Constitutional Privacy and Data Protection Rights within the EU' (2022) 47 European Law Review 482.

interest connected with individuality and protected by an individual right, we learn how the individual orientation of informational privacy can be connected to the conceptualisation and legal form of the individual within data protection.[463]

2.1. Foundational ideas of privacy

The legal protection of privacy and private life began in a variety of Western jurisdictions in the late 18th and early 19th Centuries. Perhaps the best-known early formulation of the right to privacy is found in the article of Warren and Brandeis in 1890, *The Right to Privacy,* in which the authors advocated for a "right to be let alone".[464] In this article, we can see the influence of earlier emerging notions of privacy in Europe. As Richardson recognises, this article built upon "seeds" in earlier English cases relating to search, seizure and the inviolability of the home, copyright, and parallel traditions emerging on the European continent.[465] Further, the creation of a "right to privacy" or to "respect for private life", although a relative latecomer in comparison to other liberal rights, can be seen to connect to the thinking of many 18th and 19th century liberal theorists who were conceiving of the relationship between the state and the individual.[466]

In this way, privacy and ideas of the private sphere represented thinking on the ordering of relationships between individuals and the state, and exercise or constraint of state power. At the same time, with the growth in the press and new photography technologies, we can see concerns arise of interferences with individuals' private lives, and a growing desire for states to intervene to protect these private lives. Thus, in the emergence of early privacy protections, ideas of individual rights were associated with notions of liberty and dignity, ideas which continue to have resonance with today's approach to EU data protection.

(a) Privacy, liberty, and rights

Notions of privacy protection can be connected to early conceptions of liberty and the state's relation to the private domain. In writings of 18th and 19th century theorists we see such ideas emerging. Before privacy as a standalone interest or right was protected, the concept of the private domain formed part of early liberal thinking. Berg observes that the issue tended to emerge through consideration of the proper role of the state in public and private domains,[467] as the private domain forms part of works of John Stuart Mill and Jeremy Bentham, though at times it is implicit rather than express.[468] These early formulations concerned a private space or domain which allowed for shelter from the scrutiny of the state.[469] Distinct from the public sphere—the proper arena of government and politics—the private sphere offered individuals a space to act freely. In this way, the private sphere becomes connected to individual autonomy, and the capacity to live free from state interference. While these early

---

[463] A number of jurisdictions, in particular, French, English and German speaking nations are considered, chosen due to limitations of scope of this chapter and because of the influence that these states had upon the supranational European approaches of the 20th and 21st centuries' privacy and data protection laws, including the GDPR.
[464] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[465] Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press 2017), 1-10.
[466] Glenn connects the emergence of the individual subject in law, reflecting the idea of a person in the image of God deriving from the Judeo-Christian tradition, to the emergence of subjective rights, which became an important instrument for broader human dignity. Glenn (n 342).
[467] Chris Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (Springer Nature Switzerland AG 2018) 28.
[468] ibid 24–25.
[469] ibid 25.

liberal theorists did not engage directly with a right to privacy, some of the earliest privacy rights in constitutional traditions in Europe did accord with similar conceptions of individual rights and individual liberty within the private domain.

The notion of privacy as protecting against state interference with the individual's private domain was adopted in the form of constitutional protections in some European states beginning in the 19th century.[470] For example, the Belgian constitution of 1831 restricted searches in homes and privacy of correspondence.[471] A variety of German efforts, as Snyder describes, sought to extend privacy rights from the 1830s.[472] Privacy rights were included in the Constitutional Charter of the Electorate of Hesse in 1831 and the Frankfurt Constitution of 1849 which sought to restrain the state from entering and searching homes and from confiscating letters.[473] The Austrian Constitution of 1867 protected the inviolability of the home and secrecy of letters.[474] The Bulgarian Constitution of 1879 protected inviolability of the person, domicile and correspondence.[475] Thus, in some European states, in the 19th century constitutional privacy rights of a variety of forms were adopted.

In the 20th and 21st centuries, privacy rights in various formulations became commonplace in national constitutions in European states, though not universal.[476] Today,[477] general protections for privacy or respect for private life are found in the constitution documents of Belgium,[478] Bulgaria,[479] Croatia,[480] the Czech Republic,[481] Estonia,[482] Finland,[483] Greece,[484]

---

[470] See Thomas J Snyder, 'Developing Privacy Rights in Nineteenth-Century Germany: A Choice between Dignity and Liberty?' (2018) 58 American Journal of Legal History 188. Erdos (n 462).

[471] Articles 10, 22. Belgium's Constitution of 1831. https://www.constituteproject.org/constitution/Belgium_1831

[472] Snyder (n 470).

[473] ibid 193, 204–205.

[474] Articles 9 and 10, Austrian Constitution of 1867. https://ecommons.cornell.edu/server/api/core/bitstreams/72052edc-e746-4adf-a397-3197154233a2/content

[475] Articles 73-77, Constitution of Bulgaria, 1879. Translation available in Herbert F. Wright (ed) *The constitutions of the states at war,* 1914-1918. (US Govt, 1919) https://archive.org/details/constitutionsofs00wrig/page/n5/mode/2up

[476] The current Austrian federal constitution does not protect privacy. Federal Constitutional Act of Austria. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.html

The Irish Constitution does not expressly protect privacy, though the right was judicially recognised as an unenumerated personal right protected by the Constitution. Constitution of Ireland/Bunreacht na hÉireann 1937 https://www.irishstatutebook.ie/eli/cons/en/html. See *McGee v Attorney General* [1973] Irish Reports 284*; Kennedy v Attorney General* [1987] IR 587.

The French Constitution of 1958 does not protect privacy. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/anglais/constiution_anglais_oct2009.pdf

The Constitution of the Italian Republic of 1947 does not protect privacy. https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf

[477] For a full systematic analysis of privacy and data protection rights across Europe, see Erdos (n 462), which was used to help construct this summary position.

[478] Article 22, The Belgian Constitution (English translation) https://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/GrondwetUK.pdf

[479] Constitution of Bulgaria, Article 32. https://www.parliament.bg/en/const

[480] Article 35, Constitution of the Republic of Croatia (consolidated text). https://www.sabor.hr/en/constitution-republic-croatia-consolidated-text

[481] Article 7(1), Charter of Fundamental Rights and Freedoms, https://www.psp.cz/en/docs/laws/listina.html

[482] S26, The Constitution of the Republic of Estonia. https://www.riigiteataja.ee/en/eli/521052015001/consolide

[483] S10, The Constitution of Finland https://finlex.fi/en/laki/kaannokset/1999/en19990731_20180817.pdf

Hungary,[485] Latvia,[486] Lithuania,[487] Luxembourg,[488] Malta,[489] the Netherlands,[490] Poland,[491] Romania,[492] Slovakia,[493] Slovenia,[494] Spain[495] and Sweden.[496] In other states, there is no general constitutional language protecting of private life or privacy, but narrower protections of the dwelling, or privacy of correspondence are seen, particularly in Denmark,[497] Germany[498] and Portugal.[499]

Supranational protections of privacy also developed in the 20th century, the Universal Declaration of Human Rights,[500] the International Covenant on Civil and Political Rights[501] and the ECHR would all contain privacy rights. Article 8 of the ECHR, which has significant impact on the EU data protection regime, formulated its protection as one's right to "respect for his private and family life, his home and his correspondence."

These constitutional and supranational privacy rights adopted sit within a liberal rights context, wherein rights are connected to the powers and duties of the state, and idea of an individual's liberty from state power within a private domain. Thus, some of the earliest

---

[484] Article 9(1), Constitution of Greece https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156 aggliko.pdf
[485] Article VI(1), The Fundamental Law of Hungary, https://2015-2019.kormany.hu/download/a/68/11000/The_Fundamental_Law_of_Hungary_01072016.pdf
[486] Article 96, The Constitution of the Republic of Latvia, https://www.saeima.lv/en/legislative-process/constitution
[487] Article 22, Constitution of Lithuania, https://www.constituteproject.org/constitution/Lithuania_2006
[488] Article 11(3), Constitution of Luxembourg https://www.constituteproject.org/constitution/Luxembourg_2009
[489] Article 33, Constitution of Malta, https://legislation.mt/eli/const/eng
[490] Article 10, Constitution of the Kingdom of the Netherlands https://www.government.nl/documents/reports/2019/02/28/the-constitution-of-the-kingdom-of-the-netherlands
[491] Article 47, Constitution of the Republic of Poland https://constituteproject.org/constitution/Poland_2009
[492] Article 26, Constitution of Romania https://www.presidency.ro/en/the-constitution-of-romania
[493] Article 16, Constitution of the Slovak Republic https://www.prezident.sk/upload-files/46422.pdf
[494] Article 35, Constitution of the Republic of Slovenia https://www.us-rs.si/media/constitution.pdf
[495] Article 18, the Spanish Constitution https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf
[496] Article 2, Chapter 1. Instrument of Government of Sweden. the Spanish Constitution https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf
[497] S72, the Constitutional Act of Denmark, https://www.thedanishparliament.dk/-/media/sites/ft/pdf/publikationer/engelske-publikationer-pdf/the_constitutional_act_of_denmark_2018_uk_web.pdf
[498] Article 10(1) Basic Law for the Federal Republic of Germany, https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html
[499] Article 34, Constitution of the Portuguese Republic https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf
[500] Article 12, Universal Declaration of Human Rights: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Every-one has the right to the protection of the law against such interference or attacks.* Article 8, European Convention on Human Rights: *(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*
[501] Article 17 of the International Covenant on Civil and Political Rights provides: *"(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks."*

approaches to privacy in Europe were conceived in the context of theorising and constitutionalising the relationship between the individual and the state in the liberal tradition, ideas which arose in a particular historical context, and national and regional differences shaped the formulation of that relationship. Privacy's legal form would evolve and differ in these emerging rights-based orders across Europe, but nevertheless, the place of privacy and private life in liberal rights-based orders is a development of note.

(b) Private life, dignity and the press

Dignitarian traditions of privacy and private life were also emerging in the 18th and 19th centuries in some European states. For example, the French Declaration of the Rights of Man of 1789 embodied an idea of human dignity founded on equality of all without distinction of rank or blood and sought to achieve such equality through a constitutional framework to secure these declared rights for its citizens.[502] At the same time, the French notion of *"la vie privée"* (private life) was emerging.[503] The idea of a private life which should be protected from the "insult" of press freedom was defended in the 18th and 19th centuries (both rhetorically and, occasionally, by duel) but primarily associated with the upper classes.[504] In France, the first constitutional protection of private life sought to extend this idea to all, as the French Constitution of 1791 acknowledged "calumnies and injuries" against acts of a person's private life as an exception to protections of press freedoms.[505] Whitman names this part of "a theatre of a *levelling up,* of an extension of historically high status norms throughout the population."[506]

In parallel, as Schwartz and Peifer note, the rights of dignity and personality were to play important roles in the development of Germany privacy protections,[507] as in German speaking nations, concepts of personality were emerging in philosophical discourse,[508] alongside the desire to accord the ordinary person the same legal treatment as nobles and other privileged members of society.[509]

Advances in photography and high-circulation media drew criticism as intrusions into private life, leading to our earliest privacy court cases. Just as Warren and Brandeis complained of

---

[502] Dupré (n 10) 41–42.
[503] Also sometimes '*la vie privée mureé':* private life behind the walls. See Wenceslas J Wagner, 'The Development of the Theory of the Right to Privacy in France' [1971] Washington University Law Review 28; Michelle Perrot and Roger-Henri Guerrand, 'Scenes and Places' in Michelle Perrot (ed), Arthur Goldhammer (tr), *A History of Private Life: From the Fires of Revolution to the Great War*, vol 4 (Harvard University Press 1990) 341.
[504] Whitman describes multiple duels occurring over the revelation of the pregnancy of the Duchess of Berry, the mother of the pretender to the French crown. James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' The Yale Law Journal 1153, 1173–1174. See also Wagner (n 503).
[505] Chapter V, Article 17: "Les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée, seront punies sur leur poursuite." 'Constitution de 1791 | Conseil constitutionnel' <https://www.conseil-constitutionnel.fr/les-constitutions-dans-l-histoire/constitution-de-1791> accessed 5 February 2021. See discussion in Whitman (n 504) 1172.
[506] Whitman (n 504) 1166.
[507] Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 65, 123. Whitman points to German personality rights and dignitarian justifications of legal protections as contributing to a dignitarian culture of privacy in Europe. Whitman (n 504) 1173.
[508] Whitman (n 504) 1181–1186; Richardson (n 465) 7–8.
[509] Snyder (n 470) 197–198.

the invasion of the "sacred precincts of private and domestic life",[510] many European courts were entreated to restrain such invasions, often by celebrities of the day.[511] From a small sample, a variety of legal approaches to protect private life are seen. In England, *Prince Albert v Strange* concerned the copying and proposed exhibition of etchings made by the Prince and Queen Victoria.[512] The Prince was successful, for the etchings were "subjects of private and domestic interest",[513] and the Lord Chancellor determined that "privacy is the right invaded" an immediate injunction is warranted.[514] In France, the sale and publication of a photograph of author Alexandre Dumas in his shirt sleeves with a young actress was restrained: the alienation of *la vie privée* required a formal agreement, which was absent.[515] By contrast, in Germany, personality rights were slower to extend to such occurrences, as Schwarz and Peifer note by reference to a finding of the Reichsgericht that there was no personality right violation by publication of letters written by Wagner.[516]

Thus, another tradition of privacy can be seen as associated with or sharing conceptual foundations with dignitarian approaches to private life, and ideas of a state's duty to protect its citizens equally. Individual autonomy is also understood to be central to this perspective, but by contrast to the liberal tradition, in the dignitarian vision, the individual is thought to be entitled to live freely without scrutiny by their fellow man. Such ideas are still seen in legal protections today, including in supranational privacy law. It has contributed to national legislative regimes which in turn shaped the EU data protection regime.[517] For instance, we see the ECtHR use Article 8 of the ECHR to examine violations of human dignity, though it does not appear to have so done in any informational privacy cases to date.[518] The GDPR refers to dignity only in the context of data processing relating to employment[519] and there is an ongoing scholarly debate on the proper conceptual place of dignity in EU data protection law.[520]

2.2. Privacy rights and data protection law

While a complete history of the origins of the right to privacy or respect for private life is beyond the scope of this thesis, this brief considerations of some early approaches to the protection of privacy illustrates some points of note.

---

[510] Warren and Brandeis (n 464) 195. However, despite Warren and Brandeis' concern for press intrusions into private life, the right to be let alone had little immediate effect on US privacy laws. William L Prosser, 'Privacy' (1960) 48 California Law Review 383, 384. Rather, the right to privacy in the United States is primarily still concerned with liberty from state intrusions, while a series of state tort laws developed to protect against certain intrusions of privacy. Whitman (n 504) 1161; Prosser.

[511] See Richardson (n 465).

[512] *Prince Albert v Strange* (1849) 1 Mac & G(25) 1171

[513] ibid 1172.

[514] ibid 1179

[515] *Dumas c Liébert (1867)* cited and translated by Richardson (n 465) 67, 149.

[516] Paul M Schwartz and Karl-Nikolaus Peifer, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?' (2010) 98 California Law Review 64, 1948.

[517] In particular, the German approach to data protection. See Schwartz and Peifer (n 516); Lynskey, *The Foundations of EU Data Protection Law* (n 86) 94–95.

[518] See, for example: *Pretty v. United Kingdom* App no 2346/02 (ECtHR, 29 April 2002); *A-MV v Finland* App no 53251/13 (ECtHR, 23 March 2017); *Beizaras and Levickas v. Lithuania* App no. 41288/15 (ECtHR, 14 January 2020).

[519] Article 88(2), GDPR.

[520] See Lynskey, *The Foundations of EU Data Protection Law* (n 86) 95–106; Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307; Anne de Hingh, 'Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation' (2018) 19 German Law Journal 1269.

First, privacy conceptions have been diverse from their origins, and these conceptions have ideological roots, particularly in notions of personhood and individual rights emerging in the Enlightenment. Different national traditions and experiences contributed to differing notions of privacy and protective approaches being adopted legally. Early constitutional approaches varied, with some protections focussing on the home and correspondence. Some early judicial cases looked to intrusions of the press into the domestic and intimate. These concepts of privacy embodied ideas: of the home centred around a traditional family, of the domestic sphere of women, of private property rights at the centre of the legal and political order.[521] While such ideas cannot be said to represent all historic approaches to privacy or private life in Europe, nevertheless, the existence of diverse conceptions does illustrate that differing perspectives on privacy have long existed and that such perspectives can be contextualised in broader political and cultural perspectives.

Second, these early conceptions of and approaches to privacy protections resonate today. Descendent privacy laws and national traditions of privacy also bear ideas of the private domain, individual liberty and individual dignity. Further, the ideas which informed early conceptions of privacy have generated important critiques and responses to privacy laws and scholarship.[522] Mainstream privacy and data protection scholarship can often focus on the technologies of the present and the social consequences felt in the moment, but by reflecting upon the historical and ideological origins of current regulatory strategies we can question why and how choices were made, or when assumptions and ideology have been embedded within our legal rules and institutions, and thus we are empowered to rethink established positions.

Moreover, many of these privacy rights continue to apply. Privacy and data protection laws overlap,[523] and individual rights to privacy/respect for private life and data protection are also an important aspect of data protection law.[524] Article 8 of the ECHR, and the body of decisions of the ECtHR regarding the application of Article 8 to data processing issues has become a particularly important source of data protection law, both in terms of positive and negative obligations of states. Amongst other things, Article 8 of the ECHR has been the basis of decisions regarding permissible processing of financial information,[525] health data,[526] cellular and DNA data,[527] various types of communications data,[528] permissible

---

[521] Perrot and Guerrand (n 503).

[522] For example, the feminist critiques of privacy (including the foundational works of Anita L Allen, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield 1988); Catharine A MacKinnon, *Toward a Feminist History of the State* (Harvard University Press 1989). Further important critiques are founded on critical race theory. For example: Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press 2015); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018); Ruha Benjamin, *Race after Technology : Abolitionist Tools for the New Jim Code* (Polity Press 2019).

[523] See section 3 below.

[524] See Chapter 2, section 3.1.

[525] *MN and Others v San Marino* App no 28005/12 (ECtHR, 7 July 2015).

[526] E.g. *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997); *Radu v Moldova* App no 50073/07 (ECtHR, 15 March 2014).

[527] *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008); *Gaughran v United Kingdom* App no 45245/15 (ECtHR, 13 February 2020).

[528] E.g. *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017); *Benedik v Slovenia* App no 62357/14 (ECtHR, 24 April 2018).

forms of surveillance,[529] and even the determination that Article 8 protects a form of informational self-determination.[530]

When the EU adopts its data protection regime, diverse national and supranational approaches to privacy will influence and overlap with EU data protection law. As discussed below, the grafting of the diverse ideas of privacy into an omnibus regime arguably leads to a somewhat fragmentary EU approach. Moreover, the focus upon the technocratic elements of data governance has changed the nature of the debate about data protection and privacy matters. The adoption and expansion of the data protection regime has often moved the underlying conceptions of privacy and the individual's interest in privacy—and the philosophies or ideologies which these conceptions represent—beyond question or debate. Rather, these diverse conceptions are combined and subsumed into a unitary regime, and the discussion often moves from the rationale of the regime to the detail of its formulation.

Significantly, from the outset, privacy has been concerned with the individual, a particular construction of personhood, and ideas of that individual and their place with the legal and political order. Sometimes, with rights-based approaches founded on an individual's liberty, it has represented an understanding of the relationship of the individual to the state: a domain where individuals might find shelter from state interference. In this tradition, an individual's autonomy is to be secured against the state which might constrain their ability to live freely. In some cases, this has translated to an emphasis on protection of the homes, or their domestic or intimate spheres of life.[531] In other traditions, it has represented a notion of the duty of the state to uphold the dignity of all individuals, and in these cases the state must act to secure an individual's autonomy, to act freely without intrusion. As González Fuster has written, this dignitarian perspective has also contributed to an understanding of privacy linked to individual self-determination,[532] a concept which has strongly influenced the GDPR.

Moreover, the idea of privacy as an individual interest is likely to have influenced the framing of data protection legislation in terms of individual interests. Characterising privacy as an individual interest accords with the shift towards the modern vision of the individual as the "basic social unit"[533] which was well underway when these concepts were emerging. This individualised approach has persisted. While there have been group or collective conceptions of privacy,[534] these have largely not been legally recognised. Moreover, normative calls for recognition of group or collective conceptions are framed as responses to

---

[529] E.g. *Peck v United Kingdom* App no 44647/98 (ECtHR, 28 January 2003); *Perry v United Kingdom* App no 63737/00 (ECtHR, 17 July 2003); *Antović and Mirković v Montenegro* App no 70838/13 (ECtHR, 28 November 2017).

[530] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR, 27 June 2017).

[531] Such a construction has been criticised by feminist scholars who argue that this has sheltered domestic abuse from the scrutiny of law. Arguably, the legacy of such thinking in seen in the inclusion of an exemption from regulation for purely personal and household activities. Damien Chalmers has suggested that this exemption reflects a notion of the private sphere. Damien Chalmers, 'Informational Self-Determination, EU Law and Informational Capitalism' (Centre for European Legal Studies Webinar, 27 January 2021) <https://www.youtube.com/watch?v=_TaFB78yt7A> accessed 16 February 2021.

[532] González Fuster, (n 136) 23.

[533] Siedentop characterises this transformation as marking the shift to modernity. Siedentop (n 12) 337.

[534] For example, even Westin's conception of informational privacy encompassed also a group interest, but his individual conception and the concept of informational self-determination seems to have had a longer legacy.

overly individualistic privacy law,[535] illustrating the persisting mainstream nature of an individual understanding of privacy.

As we shall see, these approaches to and conceptions of privacy and of the individual are also evident in the current EU data protection regime, and for this reason we should remember the historical and conceptual ties between the right of privacy or respect for private life and data protection law. At this point, I depart from a generalised notion of privacy, to focus on the development of informational privacy and data protection. I do so, because as once informational privacy is born, as Roessler notes, despite "diverse discourses and theoretical approaches" to privacy, "[t]he treatment of informational privacy… almost always runs parallel to and independent of these other discourses."[536] Thus, this distinct body of law and theoretical tradition is worth particular consideration.

3. From privacy to data protection

Informational privacy and data protection developed in the mid-twentieth century. As Erdos describes, after the second world war, when most European constitutions contained some form of privacy protection,[537] comprehensive regulatory frameworks constraining information did not yet exist.[538] Much as photography and telephone technologies had shaped early laws and conceptions of privacy, in the 1960-1970s, new computing technologies inspired modern informational privacy and data protection.[539]

3.1. The birth of privacy regulation

Two early influential works of the 1960s demonstrated disparate understandings of privacy and desirable approaches to privacy law, but agreed on the need for strengthened privacy laws due to technological developments.[540] Westin's foundational work, *Privacy and Freedom*,[541] though situated in the US, resonates with European approaches.[542] His approach to privacy is rooted in self-determination, defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what

---

[535] For example, Floridi, 'Open Data, Data Protection, and Group Privacy' (n 340); Mantelero (n 98); Regan (n 45); Beate Roessler, *The Value of Privacy* (Polity Press 2001); Solove, 'Privacy Self-Management and the Consent Dilemma' (n 45).

[536] Roessler (n 535) 4.

[537] In variable forms, often later subsumed into an umbrella right of privacy. González Fuster (n 136) 24.

[538] Erdos (n 136) 36. See also Erdos (n 462).

[539] Bygrave has written of the influence of new computing technologies on the mid-twentieth century discourses out of which data protection emerged. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 18) 93.

[540] Bloustein argues that "analysis of the interest involved in the privacy cases is of utmost significance because in our own day scientific and technological advances have raised the spectre of new and frightening invasions of privacy." Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962, 963. Similarly, Westin, writes that "[s]ince World War II, spurred primarily by wartime development and government projects in the cold-war era, a series of scientific and technological advances has taken place that threatens the classic American equilibrium on privacy, disclosure, and surveillance." Alan F Westin, *Privacy and Freedom* (2018 edn, Ig Publishing 1967) 66.

[541] Westin (n 540).

[542] The cross-pollination of ideas between the US and Europe is evident from parallel approaches in the US Fair Information Practice Principles and later European approaches. 'Records, Computers and the Rights of Citizens' (US Department of Health and Human Services 1973) <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> accessed 16 February 2021. See Schwartz and Peifer (n 516); González Fuster (n 136) 37.

extent information about them is communicated to others."[543] Westin suggests that privacy allows individuals to self-realise,[544] to allow individuals to determine the appropriate amount of privacy to serve their social and individual needs.[545] Moreover, as González Fuster recognises, by placing *information* at the core of his work, Westin was foundational in the birth of "informational privacy" as a distinct concept and, eventually, a field of scholarship.[546] Bloustein's position, though less cited today, presented an alternative vision of privacy, rooted in human dignity.[547] An intrusion of privacy, Bloustein writes, may threaten liberty, but "[t]he injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered."[548] Both conceptions pervade today, and both are notable for pointing to the social value[549] and group perspectives[550] of privacy, perspectives which have only more recently re-emerged.

In Europe, supranational organisations, responding to these same technological advances, began to call for strengthened protections. In 1968, the Parliamentary Assembly of the Council of Europe recommended a study on whether member state laws adequately protected the right of privacy in light of new scientific and technical methods, noting that some member states were planning to revise their legislation on this subject.[551] Throughout the 1970s, both the Council of Europe and the European Community began calling for legal reform and work on determining appropriate legal protections, with the European Community noting that "[i]t would be better for the Community to seek a genuine political consensus on this matter now with a view to establishing common ground rules, than be obliged to

[543] Westin (n 540) 24.
[544] ibid 44.
[545] ibid 45.
[546] González Fuster (n 136) 31.
[547] Bloustein (n 540).
[548] ibid 1003.
[549] ibid 1005.
[550] Westin (n 540) 36.
[551]'Human Rights and Modern Scientific and Technological Developments' (Council of Europe 1968) Assembly Debate on 31st January 1968 (16th Sitting) Recommendation 509 <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en> accessed 8 February 2021, paragraph 8 provides: *Recommends that the Committee of Ministers instruct the Committee of Experts on Human Rights: 8.1. to study and report on the question whether, having regard to Article 8 of the Convention on Human Rights, the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods; 8.2. if the answer to this question is in the negative, to make recommendations for the better protection of the right of privacy*.

harmonise conflicting national legislation later on.[552] And indeed, many European states began adopting data protection legislation from the 1970s.[553]

Two key instruments derive from the 1980s and 1990s. After a series of resolutions which considered Article 8 of the ECHR insufficient to protect against computing technologies impact on informational privacy,[554] in 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"),[555] effective in 1985.[556] The Convention is framed by a desire to extend rights protections "in particular the right to the respect for privacy" while also committing to freedom of information.[557] In the Convention, key elements of the GDPR are found: the threshold concept of personal data, defined in terms of the individual data subject; the data protection principles; data subject rights; rules regarding special categories of data, data security and data transfers across borders.[558] The ECtHR's development of a body of decisions concerning information privacy and data protection has developed in part in association with Convention 108. For example, in *Amann v Switzerland,* the ECtHR confirmed that the broad interpretation of "private life" corresponded with that of Convention 108 and the definition of personal data therein.[559]

The Data Protection Directive builds upon Convention 108, drawing upon national traditions to further articulate the duties of data controllers, rights of data subjects and enforcement methods. The legacy of national traditions of rights and individual liberty is evident in some of the legislative history seen in the development of the Directive. In advocating for limiting the scope of the Directive to natural persons, the Council Working Party noted that "it was argued that the legal philosophy underlying the directive was one of human rights and the

---

[552] 'Community Policy on Data Processing' (Commission of the European Communications 1973) Communication of the Commission to the Council SEC(73) 4300 final 13 <http://aei.pitt.edu/6337/1/6337.pdf> accessed 8 February 2021; ; 'Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector' (Committee of Ministers of the Council of Europe 1973) Resolution (73) 22 <https://rm.coe.int/1680502830> accessed 3 December 2023; 'Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector' (Committee of Ministers of the Council of Europe 1974) Resolution (74) 29 <https://resources.law.cam.ac.uk/cipil/travaux/1974%20-%20Resolution%2074(29)%20on%20Privacy%20EDB%20&%20Public%20Sector.pdf> accessed 12 February 2021 'Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing' (European Parliament 1979) OJ C 140/34 <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1979%20-%20European%20Parliament%20Resolution%20on%20DP.pdf> accessed 12 February 2021;

[553] Including the Swedish *Dataleg* (1973); the West German *Bundesdatenschutzgesetz* (1977); the Austrian *Bundesgesetz über den Schutz personenbezogener Daten* (1978); the Danish *Lov om private register* and *Lov om offentlige myndhigeders register* (1978); the French Act No. 78-17 (*loi relative à l'informatique, aux fichiers et aux libertés*) (1978); the Norwegian Data Registers Act (1978); and the Luxembourgish *Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques* (1979). See González Fuster (n 136) ch 3.

[554] See discussion in González Fuster (n 136) 83–86.

[555] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

[556] Though of course, the ECtHR would go on to develop a body of cases under Article 8 which is also an important source of data protection law and norms, often decided in association with Convention 108.

[557] Preamble, Convention 108.

[558] Article 2(a), Article 5, Article 8, Articles 6, 7, 12, Convention 108.

[559] *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000), para 65.

protection of individual freedom whereas the philosophy regarding legal persons was more concerned with questions relating to business law, professional secrets, etc."[560]

One notable tension seen in the development of EU data protection legislation is the relationship between economic objectives and the protection of individuals. The Commission, in the legislative process leading up to the adoption of the Data Protection Directive, noted that the Convention "leaves open a large number of options for the implementation of the basic principles it contains" and that "[t]he diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market."[561] Interestingly, during the legislative process, the Irish and Belgian delegations asked for the an opinion on the market harmonisation legal basis proposed "[a]s the protection of data was considered as a human rights issue".[562] The Data Protection Directive is expressly framed as an instrument to serve two objectives: the free transfer of personal data within the EU and to protect "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[563] Notably, *privacy* of personal data was still framed as a central objective.[564]

By contrast, in the GDPR, a desire to shape an autonomous identity for data protection has led to a murky relationship between privacy and data protection. When the Commission proposed the reform of EU data protection law in 2010, it cited the new Charter right to data protection as a new basis for the adoption of "comprehensive and coherent legislation on the protection of individuals with regard to the processing of their personal data and on the free movement of such data."[565] Even from the outset, there has been a lack of clarity on the relationship between notions of privacy and data protection, and their interaction in EU data protection legislation, but we shall see, in separating data protection from privacy, individual control of data will come to the fore.

3.2. Control theories of informational privacy and influence upon data protection

Where privacy might be over-theorised at an abstracted level, in data protection a different phenomenon is seen—the intricacies of a complex legislative regime take unusual primacy in the conception of the right to data protection. As Erdos recognises, data protection is distinct from traditional liberal rights: from the outset "primarily articulated as a detailed regulatory code".[566] Its status as a fundamental right in the EU came later, in 2007,[567] fifteen years after the Data Protection Directive was drafted and five years after complementary

---

[560] The Council, Outcome of Proceedings of Working Party on Economic Questions (Data Protection) on: 27 and 28 March 1991. 5705/91 Restreint Eco 39, 2.
[561] Commission Communication on the protection of individuals in relation to the processing personal data in the Community and information security. COM(90) 314 final – SYN 287 and 288. 13 September 1990, 2, 4.
[562] The Council, Outcoming of Proceedings of Working Party on Economic Questions (Data Protection) on: 25 February 1991. 5207/91 Restreint Eco 32. 14 March 1991, 12.
[563] Article 1, Data Protection Directive.
[564] Interestingly, concern was expressed by the Council Working Party that the notion of "privacy of individuals" was too restrictive, and they suggested that "the term "interests of individuals" or "individual rights"" be adopted. The Council, Outcoming of Proceedings of Working Party on Economic Questions (Data Protection) on: 25 February 1991. 5207/91 Restreint Eco 32. 14 March 1991, 20.
[565] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM/2010/0609 final. 4 November 2010.
[566] Erdos (n 136) 35. Though certainly a regulatory code which incorporated ideas of and scope for the balancing of rights and interests.
[567] Article 8, EU Charter.

electronic communications privacy legislation, the ePrivacy Directive, was adopted. As Lynskey writes, the EU failed to explain the content of the right to data protection,[568] and accordingly, the legislative form has been influential in the theorisation of the right, rather than vice-versa. In this section, I consider the way in which control theories of informational privacy have shaped and informed data protection theory.

(a) Disentangling data protection and privacy

While some historic connection between privacy and data protection is evident, once the right to data protection gains standalone status under the Article 8 of the Charter, considerable disagreement exists as to the relationship between data protection and privacy or private life, both legally and conceptually. After the creation of the standalone right to data protection, all mentions of privacy are excised from the GDPR.[569] Further, the CJEU tends to consider the rights to data protection and respect for private life together, and Lynskey and González Fuster both observe, in doing so usually conflates the rights.[570]

Scholars have sought to reconcile the rights, with differing results. Some writers have taken a formal legal approach, by comparing respect for private life under the European Convention on Human Rights with EU data protection. Differences in scope are seen; data protection is broader in applying to more types of information (without an interference with one's private life necessary).[571] While this identifies a difference in their application, it does not resolve the conceptual relationship between the two rights, nor of the nature of the right to data protection.

When it comes to discerning the nature of the right to data protection, without clear signals from legislative language or the CJEU, scholars tend to resort to inference. Gellert and Gutwirth suggest the right to data protection should be understood by reference to the processing conditions within the legislative regime, and "fair processing" principles, stating that the right to data protection can be understood "as the regulation and organisation of the conditions under which personal data can be lawfully processed."[572] Bieker makes a similar case, pointing to the principles as comprising the core of the structural element of the right to data protection.[573] Kokott and Sobotta look to the text of Article 8 of the Charter itself to emphasise that personal data must be processed *fairly* and in accordance with a legal basis.[574] Lynskey also draws on the legislative order to inform her conception of the right to data protection, observing that while the rights to respect for private life and data protection overlap, the right to data protection offers greater individual control rights over more types of

[568] Orla Lynskey (n 359) 572.
[569] Whereas the Data Protection Directive makes many mentions of the right to privacy, in the GDPR all references have been erased and replaced with references to data protection. In the Explanatory Memorandum to the Commission's initial GDPR proposal, the right to data protection is foregrounded as the relevant fundamental right, though the Memorandum does note that "Data protection is closely linked to respect for private and family life." Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD).
[570] Gloria González Fuster, 'Fighting For Your Right to What Exactly - The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection' (2014) 2 Birbeck Law Review 263; Lynskey (n 359).
[571] Gellert and Gutwirth (n 359); Kokott and Sobotta (n 359); Lynskey (n 359).
[572] Gellert and Gutwirth (n 359) 525.
[573] Bieker (n 70).
[574] Kokott and Sobotta (n 359).

information,[575] and she links this instrumental role to a normative justification for control based approaches linked to individual data harms.[576] By contrast, Purtova argues that data protection's conception derives from privacy, writing that that the right to data protection "lacks clarity as to its content and own normative weight needed in order to function as a benchmark…", thus "[i]f privacy and related autonomy and informational self-determination are not the rationale of the right to data protection … then what is?"[577]

(b) Control narratives of data protection

The dominant conceptual articulation of the right to data protection, and the purpose of data protection law, is that it intends to grant an individual control over their personal data. While this idea of data protection as the right to control one's personal data has some basis in the legislative framework, and its roots in German approaches to data protection, its dominance is less straightforward than it might appear.

The principle of informational self-determination was cemented in German constitutional law in 1983, and is a legacy of the German dignitarian conception of the personality right.[578] Efforts to explicitly adopt this principle into EU data protection law at the legislative drafting stage failed. As Purtova has described, attempts to normatively anchor the Data Protection Directive explicitly in informational self-determination fell short, though the influence of German data protection laws which were so rooted pervaded.[579] Notably, the legacy of this principle is seen in the procedural protections put in place to protect individual choices regarding data.

The Data Protection Directive did not refer to the idea of control, but rather commentators pointed to the nature of the data rights granted to individuals,[580] certain data principles[581] and the central role of consent.[582] Curiously, as the GDPR simultaneously resiles from aspects of individual control (a reduced role for consent in particular),[583] it also introduces the concept of control over one's data explicitly for the first time.[584] But notably, the GDPR never defines control over personal data as the primary objective or the core of data protection.

Lynskey's articulation of individual control over personal data interprets the legislative grant of data rights through a normative lens, as set out in the previous section. Her approach is mirrored by many. We see Purtova refer to privacy and informational self-determination as

---

[575] Lynskey (n 359).
[576] Lynskey, *The Foundations of EU Data Protection Law* (n 86) ch 6.
[577] Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86) 11.
[578] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review 84.
[579] Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86) 7.
[580] Clifford and Ausloos (n 432); Lynskey, 'Delivering Data Protection' (n 249).
[581] Purtova points to purpose limitation in particular, as "rooted in the values of informational self-determination and individual control". Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86) 14.
[582] Bietti points to the inclusion of consent in Article 8 of the Charter to argue that "the right to have control over one's personal data is implied in the right to protection of personal data" Bietti (n 86) 2.
[583] See Article 7, GDPR, which limits the use of consent to justify processing. The introduction of the accountability principle also seemingly indicates a desire to shift responsibility to controller compliance.
[584] Recital 7, GDPR: "Natural persons should have control of their own personal data." See also, Recital 75, referring to of loss of control over personal data as a risk to rights and freedoms of natural persons against which data controllers are to guard; and Recital 68.

the “normative anchors” of the Data Protection Directive.”[585] She suggests breaking the link between privacy and data protection “would amount to breaking the normative connection between data protection and informational self-determination.”[586] Ausloos argues that control over one’s personal data is “the essence” of the right to data protection,[587] though this seems to be a normative claim rather than a doctrinal one.[588]

Even those who criticise individual control usually take it as the starting point.[589] For example, Bernal advocates for informational privacy grounded in autonomy and collaborative consent, while critical of prevalent consent practices and consent under the Data Protection Directive.[590] Further, Bietti points to EU data protection “grounded in the normative intersection of control, consent, and choice” while advocating for a move away from discourses of individual control over data, and recourse to less ‘individual control-centric’ provisions, such as DPIAs and data protection by design and default.[591] Koops argues that the focus upon individual control of information denies the reality of modern data processing.[592] For Hartzog, “an empire of data protection has been built around the crumbling edifice of control.”[593]

As this literature suggests, there are challenges with a conceptualisation of a right or legislative regime around a notion of individual control when that element of control is implicit rather than explicit in the regime. As Lynskey has pointed out, there is “no single ‘principle of control’ in EU data protection legislation.”[594] There have been few attempts to articulate what control of one’s data might mean beyond the exercise of the given rights and consent. Ausloos proposes control as “a fluid concept”, with a positive and negative dimension—an individual must be able to manifest their choices over data use and at the same time should be protected from their autonomy being subverted.[595]

Others have drawn upon the ideas which informed early privacy laws, in particular rooting self-determination in theories of autonomy beyond informational control. Rouvroy and Poullet advocate for a virtue ethics informed vision of respecting autonomy: to allow individuals to develop capacities for deliberative autonomy and for collective deliberative autonomy, and to

---

[585] Purtova, ‘Default Entitlements in Personal Data in the Proposed Regulation’ (n 86) 9, 18.
[586] ibid 9.
[587] Ausloos (n 84) 61.
[588] Scholarship on the essence of Article 8 suggest the essence has not yet manifested as a coherent concept. Maja Brkan, ‘The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning’ (2019) 20 German Law Journal 864; Maria Grazia Porcedda, ‘On Boundaries -Finding the Essence of the Right to the Protection of Personal Data’ in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019).
[589] Including Lynskey, see Lynskey, *The Foundations of EU Data Protection Law* (n 86) ch 7.
[590] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) ch 2.
[591] Bietti (n 86) 4.
[592] Bert-Jaap Koops, ‘The Trouble with European Data Protection Law’ (2014) 4 International Data Privacy Law 250, 251.
[593] Hartzog (n 310) 425.
[594] Lynskey, *The Foundations of EU Data Protection Law* (n 86) 180. This was recently echoed by Advocate General Campos Sánchez-Bordona who notes that “The GDPR does not include a precise definition of ‘control’ (and I have not found one anywhere else either).” C-300/21 *Österreichische Post AG* Opinion of Advocate General Campos Sánchez-Bordona 6 October 2022 (ECLI:EU:C:2022:756), para 70.
[595] Ausloos (n 84) 64.

live a self-determined life.[596] Kosta builds on this analysis to ground her normative conception of consent as "an act of autonomy".[597]

Setting aside for future discussion the merits of individual control based approaches to data protection,[598] at this point, I suggest that the understanding of data protection as individual control over data is not inevitable. As Purtova has written, whether individual control over data should be the defining normative choice underlying EU data protection was a choice that the EU legislature were facing upon the adoption of the GDPR.[599] While Purtova was characterising this as a choice between individual control based approaches and the entitlement of data processors to use data, we can extend her point. While Article 8 of the Charter prescribes that the EU protect the right to data protection, it does not prescribe how such data protection should be conceived, beyond fair and lawful processing (by consent or otherwise), the right to access and supervisory authorities. However, we should recall that various ideas and traditions have informed the GDPR, which is a product of political choices and compromise, based on assumptions of how control might contribute to individual wellbeing. If doubts exist as to whether it is in fact making such a contribution, we can question and revisit this approach. We can look to deeper accounts of autonomy, such as Rouvroy and Poullet's vision, to examine how data protection can contribute to individual autonomy, rather than taking for granted that individual control over data choices serve those ends.

3.3. From state power and duty to individual autonomy and fairness

If we contrast these conceptions of the right to data protection to that of its legal and conceptual relation—privacy—an interesting phenomenon is observed.

Rights to privacy and respect for private life can be linked to two parallel conceptual traditions, concerned with the right to liberty from the coercive power of the state, and the duty of the state to protect from invasions into one's domestic and intimate sphere. The early liberal rights order in which some European privacy rights were incubated was concerned with power imbalances: the coercive power of the state and the state's duty to intervene to constrain invasive new technologies.

Modern concerns about state and organisational surveillance are not so different. Yet under the GDPR, the debate is framed differently. Discussions of power are largely absent,[600] and instead interests are "balanced", through the language of fairness, individual self-determination and in public contexts, proportionality. People have been homogenised into the archetypal individual data subject or natural person, and questions of power have been silenced as they were subsumed into a governance framework premised upon a liberal rights regime.

Yet, traditional liberal rights frameworks are critiqued from many angles—as Graziadei has written—their illusory nature to the disenfranchised and marginalised, for their idealised

---

[596] Rouvroy and Poullet (n 310) 14.
[597] Kosta, *Consent in European Data Protection Law* (n 229) 140.
[598] See Chapter 5.
[599] Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86).
[600] A number of scholars have advocated for inclusion of such power dynamics. See e.g. Orla Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 Theoretical Inquiries in Law 189; Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27).

models, and the failure of the language of individual rights to capture the social.[601] When we recognise that the discussion has been framed by a 19th century vision of legal solutions to privacy issues, we can also examine how alternative responses to these liberal framings can illuminate our responses to the challenges we face.[602]

Of course, data protection may be understood in part in light of liberal ideas of privacy or private life, but it does so in a particular supranational context. Therefore, to more fully grasp some of the ideas which underpin data protection, we cannot ignore the relevance of the EU's political and institutional character.

4. The EU and the individual in data protection law

While the previous section has argued that the GDPR has many historical antecedents which contributed to or interact with it, at the same time, the EU context of the data protection project has also shaped the manner in which data protection is designed and practised.[603] Inspired by the suggestion that the individual's conception in EU law cannot be separated from the institutional context which informs that conception,[604] this section explores how the institutional and political context of the EU shapes the role and conception of the individual within EU data protection law. I argue that the institutional, political and legal order of the EU has significantly shaped the GDPR, depoliticised some of the choices underpinning the regime and has contributed to a fragmentary vision of the individual within EU data protection law. I suggest that there are competing ideas of the individual within the law, and explore one particular tension: the contrasting implications of conceiving of the individual as a rights-holder within the EU project, and the individual as a consumer in the EU single market.

4.1. The EU and the individual

There are many reasons why the EU context is relevant to an analysis of the role and conception of the individual within EU data protection law. The first is simple: the GDPR is an EU legislative act. The Data Protection Directive was adopted as a market harmonising measure. Persistent variation due to national variations in transposition was put forward as one of the justifications for adopting an EU Regulation to replace the Directive, the GDPR.[605] For this reason, Lynskey suggests that the GDPR would lead to the "Europeanisation" of data protection law, in the establishment of a centralised EU approach to data protection law.[606] While the GDPR, in name a Regulation, still allows for Member State variation and implementation in a number of areas,[607] it has narrowed divergence.

---

[601] Michele Graziadei, 'Rights in the European Landscape: A Historical and Comparative Profile' in Sacha Prechal and Bert van Roermund, *The Coherence of EU Law: The Search for Unity in Divergent Concepts* (Oxford University Press 2008) 86–87.

[602] See a similar argument in Julie Cohen, 'Studying Law Studying Surveillance' (2014) 13 Surveillance & Society 91.

[603] Lynskey has argued for the need to place the GDPR and data protection law more broadly within its EU context. See e.g. Lynskey, *The Foundations of EU Data Protection Law* (n 86); Orla Lynskey, 'The "Europeanisation" of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252; Orla Lynskey, 'Extraterritorial Impact in Data Protection Law through an EU Law Lens' in Federico Fabbrini, Eduardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing 2021) <https://www.ssrn.com/abstract=3674413> accessed 29 October 2020.

[604] Azoulai, Pataut and Barbou des Places (n 123) 4.

[605] Recital 13, GDPR.

[606] Lynskey, 'The "Europeanisation" of Data Protection Law' (n 603).

[607] Recital 8, GDPR.

Moreover, the CJEU has taken on an increasingly significant role in the interpretation of data protection law since the adoption of the Charter in 2007.[608] The individual is said to be at the heart of the European Union project[609] and the adoption of a right to data protection has had a significant impact in the case law of the CJEU.

Data protection has also become connected to the external political activities of the EU, as trade agreement negotiations incorporate assessments of third country data protection regimes in order to facilitate data transfers. This has resulted in many countries adopting legislative regimes which are informed by EU standards.[610]

By situating the understanding of the subject in its EU context, a deeper understanding of the notional individual within the regime is possible. In the case of the GDPR, this allows us to understand how the place of the individual within the EU project has influenced the design and operation of the GDPR, and the particular role that the individual plays within the law. In earlier works on the notion of the individual in the EU, two important aspects of this context inform EU data protection law.

First, the particular legal and political order of the European Union has shaped the role and conception of the individual within the EU legal order. The unique nature of the EU as a supranational project, with limited allocated competences and challenges of legitimacy, has led to placing of the individual at the centre of the European Union project.[611] Thus, the individual is placed in the middle of debates on the legitimacy of the EU.[612] The individual has also played an important operational role in realising the Union through the exercise of individual rights.[613]

But because of the piecemeal nature of the regulatory spaces in which the EU operates, a fragmented and sometimes contradictory conception of the individual within the EU arises. As Dani has argued; "individuals are often situated at the intersection of multiple

---

[608] Prior to 2007, there were only 9 decisions of the CJEU which cited the right to data protection or the Data Protection Directive. Since then, there have been over 70 more.

[609] Preamble, Charter.

[610] Greenleaf has traced the influence of European data protection standards globally. Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108?' (2012) 12 University of Edinburgh Research Paper Series 36; Graham Greenleaf, '"European" Data Privacy Standards Implemented in Laws Outside Europe' (2018) 18 University of New South Wales Law Research Series <https://ssrn.com/abstract=3096314> accessed 9 April 2019.

[611] Loïc Azoulai, Ségolène Barbou des Places and Etienne Pataut (eds), *Constructing the Personal in EU Law: Rights, Roles, and Identities* (Hart Publishing 2016); Weiler (n 123); Susanna Lindroos-Hovinheimo, 'There Is No Europe-On Subjectivity and Community in the EU' (2017) 18 German Law Journal 19.

[612] Somek (n 12); Floris de Witte, 'Emancipation through Law?' in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016); Floris de Witte, 'Integrating the Subject: Narratives of Emancipation in Regionalism' (2019) 30 European Journal of International Law 257.

[613] Weiler has pointed to the importance of the doctrine of direct effect in constituting the EU legal order, in part through the harnessing of individual interests in the vindication of rights owed them by national states. Weiler (n 123) 96. See also discussion of Azoulai et al on the individual as an agent of the EU. Azoulai, Pataut and Barbou des Places (n 123) 4.

Dawson and Muir have also written that the "EU law establishes a legal system that has uniquely relied on individuals to enforce, through litigation, the rights laid down in the founding EU Treaties. It is the very ability of individuals to be the bearers of rights that distinguishes the EU from most international organizations." Mark Dawson and Elise Muir, 'Individual, Institutional and Collective Vigilance in Protecting Fundamental Rights in the EU: Lessons From the Roma' (2011) 48 Common Market Law Review 751, 754.

governmental strategies with distinct and not necessarily coherent policy goals, rationales and ideologies."[614] EU law creates many classifications of individuals (worker, consumer, student etc.), and depending on the classification of the individual and "various regimes of individual action and different sets of rights" are created.[615] Further as Azoulai has written, "EU law is a conceptual world in which the individual's participation into pre-existing institutional contexts rooted within the Member States is key."[616] Thus, the individual is a worker in a workplace, a consumer in a marketplace, a member of a mobile family etc.[617] Accordingly, our understanding of the individual in EU law is deriving from multiple sites, as a set of supranational measures interact with national regimes, contexts and institutions. Unsurprisingly, therefore, how the worker, the consumer or the family member is understood in EU law differs. However, the data subject, due to the ubiquity of data processing,[618] is all of these. Therefore, multiple understandings of the individual across different categories are collapsed into a single classification when we consider the role of the individual as data subject.

Second, the EU project is premised upon the achievement of a particular socio-economic order.[619] The EU built a pluralist constitutional order, which was premised upon "the idea that the EU includes a promise of justice different from, but as valuable as, the one that nation states can achieve."[620] The Charter endorses a conception of the human being imbued with moral value, vested with "dignity, self-determination, a capacity to enjoy rights and to hold values, and a corresponding sense of responsibility".[621] But alongside this Charter of rights, the economic origins and current economic objectives have defined the EU, and this economic ideology shapes the understanding and role of the individual in the EU legal order.[622] As De Witte writes, EU economic integration "places the subject at the centre of the European project; while the objective is the need to constrain public (state) power, the main instrument to do so is the subject's economic freedom."[623] Thus, we see a constitutional order which is premised upon a particular economic model and mission, and individual rights become connected to this economic mission. Individuals acquire "[r]ights to produce, trade, acquire and exchange goods, provide services and develop all kinds of activities … [which] aim at their participation in an institutionalised marketplace."[624] The exercise of individual rights support the functioning of the EU internal market, and the building of a new socio-economic order.[625]

It is therefore unsurprising to see competition between economic and constitutional subjectivities in EU law.[626] I suggest we also see such competition in data protection law.

---

[614] Marco Dani, 'The Subjectification of the Citizen in European Public Law' (2015) 02 EUI Working Papers 35, 2. See also O'Brien (n 18).
[615] Azoulai, Pataut and Barbou des Places (n 123) 5.
[616] Loïc Azoulai, 'The European Individual and Collective Entities' in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016) 204.
[617] ibid.
[618] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86).
[619] See Azoulai, Pataut and Barbou des Places (n 123) 6.
[620] Lindroos-Hovinheimo, 'There Is No Europe-On Subjectivity and Community in the EU' (n 533) 1231.
[621] Azoulai, Pataut and Barbou des Places (n 123) 4.
[622] See O'Brien (n 18).
[623] de Witte (n 612) 264.
[624] Azoulai (n 616) 204.
[625] Azoulai, Pataut and Barbou des Places (n 123) 5–6.
[626] Dani (n 614) 18.

The GDPR, like its predecessor, seeks to combine a rights-based regime with a particular economic mission,[627] and a vision of data as an economic asset. This duality contributes to a tension between the idea of the data subject as a rights-holder and the economic vision of data processing and the status of the data subject as a market participant. But while an economic ideology informs the role of the individual at the constitutional and institutional level, at a legislative level, in the case of the GDPR, debates on the economic role of data and individuals' status as economic participants have been pre-empted by existing Union policies and priorities. By resurfacing these underlying choices, we can re-engage with vital questions on the nature of the regulatory approach.

4.2. The data subject as rights-holder, the data subject as consumer

The GDPR, although adopted solely on the basis of a legislative competence founded on the right to data protection,[628] continues to have a combined fundamental rights and economic orientation. The Regulation is intended to contribute to "economic and social progress", to both strengthen economies and to individual well-being.[629] The right to data protection is to be balanced with other rights and freedoms, including the freedom to conduct a business.[630] Technological developments should be harnessed through the free flow of data throughout the Union.[631] Compliance obligations are tailored to the needs of small and medium sized enterprises.[632]

In general, data subjects are considered in a homogeneous manner, unless they are children or in certain cases of processing special categories of personal data.[633] However, different ideas of the individual are embedded in the law which mirror the dual economic and rights goals. As a generality, one division of conception of the individual we can discern from the GDPR is between the notion of the individual as a market participant—a consumer—and the individual as a rights-holder. This distinction comes to the fore in the division between those elements of the law which apply to state processing activities in public contexts and those of the private sector.

If we look to the sections of the GDPR which govern the legality of processing data by state and public authorities, these provisions reflect the language of fundamental rights. Data processing on the basis of a legal obligation or public interest must be provided for by law.[634] Such legal measures can and have been challenged using Article 8 of the Charter.[635] Similarly, processing of special categories of personal data must accord with fundamental rights standards.[636] In the decisions of the CJEU, the fundamental rights to data protection and respect for private life have been powerful instruments for the review and invalidation of state measures, including; the Data Retention Directive,[637] two Commission adequacy

---

[627] Article 1, GDPR. Orla Lynskey has written of these dual objectives under the Data Protection Directive. Lynskey, *The Foundations of EU Data Protection Law* (n 86) ch 3.
[628] Article 16, TFEU.
[629] Recital 2, GDPR.
[630] Recital 4, GDPR.
[631] Recital 6, GDPR.
[632] Recital 13, GDPR.
[633] See further Chapter 6.
[634] Articles 6(1)(c) and (e), 6(3) GDPR.
[635] C-398/15 *Manni* (ECLI:EU:C:2017:197); C-73/16 *Puškár* (ECLI:EU:C:2017:725); Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601). See discussion in Chapter 2, section 3.2(b).
[636] Article 9(2)(h), GDPR.
[637] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of

decisions,[638] a proposed international data sharing agreement[639] and multiple national surveillance measures.[640] It is not surprising that a rights-based approach would apply to state processing activities, after all, rights emerged first in Europe in the context of questions of law and liberty from state coercion.[641]

By contrast, the language of the GDPR when oriented towards the private sector is less rights-oriented, and more economic. Some have distinguished consumer law and data protection regimes as separate and of a different character,[642] but at EU level, data protection has always had an economic character.[643] There are many aspects of the law which embody an idea of the individual as a consumer. Indeed, such complementarity has inspired some to suggest that consumer law enforcement may have a role to play in the data protection sphere.[644]

If we consider the governance of private sector processing, many of the GDPR's provisions adopt the language or strategies of economic ideas of data processing. We may point to three of the pre-conditions to lawful processing: consent, processing necessary for performance of a contract, and for the purposes of legitimate interests. Elements of consent requirements mirror a contractual vision of consent: with rules as to the presentation of consent in a written declaration,[645] or granted in the context of a contract,[646] and indications that box-ticking and internet settings are possible means of consent.[647] Special provisions are provided for the processing of children's data is in the context of information society services (by contrast to other areas central to children's rights, such as schools, childcare or sports and recreation providers).[648] This is reinforced by the existence of exceptional approaches to consent in areas outside commercial processing: special rules for broad consent to scientific research[649] and the presumption against consenting to data processing

---

publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Invalidated in joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238).

[638] C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650); C-311/18 *Data Protection Commissioner v Facebook Ireland* (ECLI:EU:C:2020:559).

[639] Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656).

[640] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970); C-623/17 *Privacy International* (ECLI:EU:C:2020:790); C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791); Case C-140/20, *Commissioner of an Garda Síochána and Others* (ECLI:EU:C:2022:258). See discussion in Chapter 2, section 3.1.

[641] See section 1 above; Graziadei (n 601) 65.

[642] Helberger et al observe the historic places of consumer and data protection law as 'different worlds'. Helberger, Zuiderveen Borgesius and Reyna (n 412). Rott characterises data protection as originating in a constitutional context and having a fundamental rights orientation. Peter Rott, 'Data Protection Law as Consumer Law – How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law' (2017) 3 Journal of European Consumer and Market Law 113. Schwartz and Peifer have suggested that the US approach to data privacy founded on an idea of consumer protection in an unfair marketplace in contrast to the European privacy culture founded on rights. Schwartz and Peifer (n 516) 119.

[643] The Data Protection Directive was adopted as a market harmonisation measure under the precursor to Article 114 TFEU.

[644] Rott (n 642); Helberger, Zuiderveen Borgesius and Reyna (n 412). Lynskey has also suggested that consumer law alongside competition enforcement could be a more holistic approach to data protection. Lynskey, *The Foundations of EU Data Protection Law* (n 86); Lynskey, 'Grappling with "Data Power"' (n 600).

[645] Article 7(2), GDPR.

[646] Article 7(4), GDPR.

[647] Recital 32, GDPR.

[648] Article 8, GDPR.

[649] Recital 33, Article 89, GDPR.

by public authorities.[650] Processing on the basis of contractual necessity invokes a bargain struck between data subject and controller. Legitimate interests processing often also invokes economic considerations: an explicit mention of the data subject as client or contractor, and designating fraud prevention and direct marketing as potential legitimate interests.[651]

Transparency as a core data principle[652] shares with consumer law "the pivotal role of information as a means to mitigate information asymmetries and to empower the individual."[653] Similarly, the right to data portability, applicable only to private sector processing,[654] demonstrates the shared idea of consumer choice as a mode of individual protection, and a hesitancy to interfere with business models grounded upon data processing. We also see parallels in the enforcement mechanisms adopted in consumer law and data protection law, including the role of national supervisory authorities.[655]

The CJEU has also expressly adopted the idea of the data subject as a consumer, or an economic participant. We see this first when it endorsed the role of consumer authorities in upholding data protection law in *Meta Platforms Ltd.*[656] In finding that a German consumer protection association might fall within the scope of the Article 80 representational action, it found that "it pursues a public interest objective consisting in safeguarding the rights and freedoms of data subjects in their capacity as consumers, since the attainment of such an objective is likely to be related to the protection of the personal data of those persons."[657] A consumer harm could be associated with data protection practices, the Court recognised finding that "The infringement of the rules intended to protect consumers or to combat unfair commercial practices … may be related, as in the present case, to the infringement of the rules on the protection of personal data of those consumers."[658] Advocate General Pitruzzella goes even further in *TU, RE v Google,* when he looks to permissible limitations to the right to erasure under Article 17 of the GDPR, to be interpreted in light of the rights to respect for private life and data protection.[659] In the weighing of private life and data protection against the right of the public to obtain information, and the right of a web page operator to inform, the Advocate General determines that one's economic status has a bearing on the extent of one's private life. The role that one plays in public life, the Advocate General finds, depends not only on public office "but also situations where he or she has a significant economic role."[660] Justified in the need for "proper functioning of the market", and the need for the availability of information in professional roles, the Advocate General states that "acceptance of an economic role entails acceptance of a limitation on the scope of protection of private life."[661] This, however, was not explicitly reiterated by the Court, which

---

[650] Recital 42, GDPR.
[651] Recital 47, GDPR.
[652] Article 5(1), GDPR and Articles 12-14, GDPR.
[653] Helberger, Zuiderveen Borgesius and Reyna (n 412) 1437.
[654] Article 20, GDPR.
[655] Notably, data protection actions have been included in the new consumer collective redress package. DIRECTIVE (EU) 2020/1828 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409/1, 4/12/2029, p 1–27).
[656] C-319/20 *Meta Platforms Ireland* (ECLI:EU:C:2022:322).
[657] ibid, para 65.
[658] ibid, para 66.
[659] C-460/20 *TU, RE v Google* Opinion of Advocate General Pitruzzella, 7 April 2022 (ECLI:EU:C:2022:271)
[660] ibid, para 28.
[661] ibid.

merely stated that “where the data subject plays a role in public life, that person must display a greater tolerance, since he or she is inevitably and knowingly exposed to public scrutiny”,[662] seemingly leaving the question of the connection between economic status and public life to the referring court.

That is not to say rights-based conceptions are absent in the GDPR’s application to private sector processing. The rights to data protection and respect for private life have shaped CJEU decisions concerning private sector processing. Perhaps the greatest innovation is the development of the right to be forgotten in *Google Spain*.[663] Otherwise, the primary impact of the rights-based objective is seen in the expansive interpretative tendencies of the CJEU;[664] including the expansion of the territorial reach of EU data protection law[665]and a broader material application of EU data protection law.[666]

Therefore, to generally contrast the impact of the right to data protection in the private and public sectors, in processing for public interest and legislative purposes, the right to data protection holds states to account by subjecting their data protection activities to a fundamental rights review (involving questions of necessity, proportionality and the essence of the rights), whereas in the private sector, the question of the horizontal application of the rights protections as an additional layer of review in addition to the legislative scheme as opposed to simply informing the operation of the legislative scheme is still an open question.

4.3. Reckoning with competing ideas of the data subject

Just as EU consumer law has been said to create a “fractured” subjectivity, where the consumer exists as “a bundle of partial identities”,[667] there are multiple ideas of the data subject within EU data protection law. I have suggested two of these understandings, which illustrate how our idea of the individual and the extent of their legal protection may be shaped by their relationship to the data controller: a rights-holding individual subjected to the powers and duties of a state, or a consumer of goods and services provided by a business. Although nominally all data processing within its scope is subject to a single regime—the GDPR—within that regime exist elements which are more relevant to different types of processing.

By acknowledging these multiple identities of the data subject, and mapping how the protections of the law extend depending on these multiple identities, I suggest new lines of investigation are uncovered. We may question how a rights-based approach should manifest in a horizontal relationship between private parties, and whether an economic vision of private sector surveillance is appropriate. We can look to consumer law theory to inform data protection—such as our ideas of what “fairness” in the data protection context may mean.[668]

---

[662] C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962) para 63.
[663] C-131/12 *Google Spain and Google* (ECLI:EU:2014:317).
[664] Discussed in Chapter 2, section 2.2(b).
[665] In C-131/12 *Google Spain and Google* (ECLI:EU:2014:317); C-230/14 *Weltimmo* (ECLI:EU:C:2015:639)*;* C-191/15 *Verein für Konsumenteninformation* (ECLI:EU:C:2016:612); C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388).
[666] C-101/01 *Lindqvist* [2003] ECR I-12992; C-212/13 *Ryneš* (ECLI:EU:2014:2428 C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551); C-582/14 *Breyer* (ECLI:EU:C:2016:779); C-434/16 *Nowak* (ECLI:EU:C:2017:994)*;* C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), par 53*;* C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388)*;* C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551); C-40/17 *Fashion ID* (ECLI:EU:C:2019:629).
[667] Marco Dani, ‘Assembling the Fractured European Consumer’ (2011) 29 LSE ‘Europe in Question’ Discussion Paper Series 4 <http://www.ssrn.com/abstract=1738474> accessed 1 December 2020.
[668] See Clifford and Ausloos (n 432).

More fundamentally, by uncovering ideological choices and assumptions which underpin the GDPR, which can derive from the socio-political order the EU pursues, we can re-engage with the desirability of these choices. By contrasting the difference between rights-based interpretations and economically led interpretations in different contexts, we may recognise an apparent assumption that private sector processing is to be regarded through a lens of market relations. The recognition of such an assumption allows us then to revisit the legitimacy and desirability of such data collection, and to ask whether the embedding of market logics is legitimising the economic use of data without public scrutiny or debate over the merits of such approaches.

5. Conclusion

Placing the individual's role and conception in historical, institutional and theoretical context allows us to appreciate some of the ways in which diverse historical, regional and cultural ideas contribute to data protection law. The individual's role within EU data protection law is a product of multiple factors, some of which are considered in this chapter. The individual's role can be connected to notions of privacy, ideas of informational self-determination and the individual's place within the European Union project, and therefore the fragmentary conceptions of the individual in EU data protection law are unsurprising. Ideas of privacy emerged in diverse traditions, some of which connected to questions of state power and individual liberty, notions of individual dignity and the state's duty to uphold the dignity of all. Concerns associated with modern computing technologies, amongst other developments, drove new generations of legislation premised on individual protection through data governance. The GDPR is a tapestry, with threads deriving from multiple nations, institutions and traditions. This chapter sought to unpick only some of these threads. This patchwork nature causes challenges when we try to identify the nature of the right to data protection in isolation. The GDPR offers us only grounds for inference. Normative arguments based on individual control have become prevalent, but I suggest by recognising that this position is a normative choice, and remembering that there have long been differing and contested conceptions of privacy, private life and data protection, we can re-engage with the notion of individual control of data.

Further, by situating the law and the place of the individual in data protection law within the wider EU context, we see that the placing of the individual at the centre of the GDPR accords with broader EU strategies and the political and institutional nature of the EU. By acknowledging the socio-economic order within which the GDPR was developed, we can situate concerns about state surveillance, informational capitalism and systemic data abuse and analyse the law's contributions to such business practices and its capacity to respond to them.

Finally, by acknowledging some of the contextual factors which can be connected to the place of the individual in EU data protection law, and recognising that our legal model of the individual is based on underlying ideas about privacy, data protection, rights and the economy, we also open up a new line of analysis. If the idea of the individual has been shaped by a range of historical, cultural and theoretical influences, we can begin to uncover and question some of these influences. This chapter does not offer a complete account of such influences, but rather seeks to unveil the possibility of recognising such influences. By tracing the conception of the individual, we have reminded ourselves that the individual in EU data protection law is a notional individual, and it can be valuable to question those notions. In other words, we can seek to uncover the theory or model of personhood which is informing the legal treatment of the individual. This line of analysis will be further considered in the subsequent chapters, as we dive more deeply into the ways in which EU data

protection law reflects ideas about the identity, relations and capacities of the individual. First, in Chapter 4, we will consider the ways in which EU data protection law balances ideas of relationality and individuation of the individual.

CHAPTER 4: THE RELATIONAL INDIVIDUAL AND PLURAL PERSONAL DATA

1. Introduction

Previous chapters have made the argument that the individual is central to EU data protection law due to their multi-faceted role within the regime, that this centrality can be contextualised by reference to the historical and institutional environment in which the law developed, and that these contextual influences have contributed to certain ideas within the law, including about the nature of individuals and personhood. This chapter extends our investigation of the notions of personhood which we find within the law, i.e. the conception of the individual within EU data protection law.

The aspect of personhood to be examined in this chapter is the question of relationality versus individuation: are persons conceived as interdependent with others or as independent individuals? In other words, this chapter investigates one element of the conception of the individual under EU data protection law: the degree to which the law recognises and can accommodate a relational understanding of the individual, and how the law contributes to the structuring of relationships. The picture which emerges is one of fragmented recognition of plurality, and a primarily individuated understanding of the person at the centre of EU data protection law, which can manifest in challenges in the application of data protection law.

1.1. Relationality and the individual

The individual at the centre of Western political philosophy, underpinning modern institutions, tends to be traced to Enlightenment thinking and theorised as a "completely self-contained being that develops in the world as an expression of its own unique essence."[669] Glenn has argued that these Enlightenment ideas of a self-standing individual were a reaction to an earlier form of relational thinking, in which the life of the serf or bonded servant was defined in hierarchical relation to their lord, and in terms of obligations owed.[670]

At much the same time as Donne offered us this meditation against isolationism; "No man is an island, entire of itself; every man is a piece of the continent, a part of the main"[671], Descartes' foundational work of philosophy was published,[672] pointing to the singular, doubting, thinking man as the source of understanding and knowledge.[673] Mansfield points to later Enlightenment thinkers Rousseau and Kant, different in their vision of the individual, but both part of the same shift of emphasis towards the individual self, and to Rosseau's "solitary walker … an emblem of this emphasis on the individual as the fundamental material of the human world."[674] Mansfield suggests that the terms of debates about subjectivity are

---

669 Nick Mansfield, *Subjectivity: Theories of the Self from Freud to Haraway* (New York University Press 2000) 13. See also discussions in Dror Wahrman, *The Making of the Modern Self: Identity and Culture in Eighteenth-Century England* (Yale University Press 2004); Glenn (n 342).
670 Glenn (n 342).
671 John Donne, Meditation XVII, 1624.
672 René Descartes, Discourse on Method, 1637.
673 Mansfield (n 669) 14.
674 ibid 21.

still founded in the debates of the Enlightenment,[675] and indeed ideas of independence versus interdependence (in a variety of framings) were recurrent themes.

Conceptions of the self shift through history,[676] and in parallel, philosophers continually debate over the nature of identity and individuality. In this chapter I do not purport to grapple with these debates, my ambitions are smaller. I reflect on one dichotomy seen in our idea of the individual—the tension between an understanding of an individual as self-contained or isolated, and that of an individual as a relational being, and more particularly, how these understandings operate in the conception of the individual in EU data protection law, and specifically the consequences for the operation of the GDPR and Article 8.

Relational understandings of personhood tend to place themselves in opposition to a notional liberal idea of personhood. Relational theory is particularly associated with feminist theories grounded in social theory, who criticise the "prominence afforded to individual autonomy in a range of theories,"[677] particularly contemporary liberalism which focuses upon formal equality and individual rights which fail to deliver equality or freedom due to a failure to address social forces.[678] Relational feminist theory has then inspired a number of works in law (particularly medical and family law) which advocate for relational approaches.[679] Relational understandings of the individual are also seen in non-Western settings. Birhane points to Ubuntu (humanity), as a contrast to the Western Cartesian idea of the self.[680] Ubuntu is a term given to an African philosophy, in Zulu: "'*Umuntu ngumuntu ngabantu*', which means 'A person is a person through other persons.'" [681]

In this chapter, I adopt Nedelsky's conception of a relational self, by which she means that human beings are fundamentally interconnected and interdependent, and individuals are constituted by the networks of relationships to which they belong, from interpersonal relationships to wider structural relationships (such as gender or class relations) and institutional relationships (such as with the global market).[682] Nedelsky's theory is developed with law in mind, and allows analysis of particular legal regimes, by asking, what structures of relationships do those regimes encourage?[683]

---

[675] ibid 22.

[676] See Charles Taylor, *Sources of the Self: The Making of the Modern Identity* (Cambridge University Press 1989); Wahrman (n 669); Nicola Lacey, *Women, Crime, and Character* (Oxford University Press 2008).

[677] Linda Barclay, 'Autonomy and the Social Self' in Catriona MacKenzie and Natalie Stoljar (eds), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000) 53.

[678] ibid 56.

[679] For example, Alasdair Maclean, *Autonomy, Informed Consent and Medical Law: A Relational Challenge* (Cambridge University Press 2009) <http://ebooks.cambridge.org/ref/id/CBO9780511576119> accessed 16 September 2021; Jonathan Herring, 'Forging a Relational Approach: Best Interests or Human Rights?' (2013) 13 Medical Law International 32; Charles Foster and Jonathan Herring, *Identity, Personhood and the Law* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-53459-6> accessed 10 August 2020.

[680] Abeba Birhane, 'Descartes Was Wrong: "A Person Is a Person through Other Persons" | Aeon Ideas' (*Aeon*, 7 April 2017) <https://aeon.co/ideas/descartes-was-wrong-a-person-is-a-person-through-other-persons> accessed 7 September 2021.

[681] ibid.

[682] Jennifer Nedelsky, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (Oxford University Press 2011).

[683] Nedelsky suggests that the relational methodology facilitates "attending to the ways in which law structures relationships, which, in turn, enhance or undermine core values." ibid 78.

1.2. Relationality and EU data protection law

Relationality has informed many works of privacy theory, as a number of scholars (predominantly writing from US perspectives) have advocated to recast privacy from an individual to a relational lens.[684] Lindroos-Hovinheimo has argued that an ideology of possessive individualism underlies EU data protection, which comes into tension when "[o]ur data is seldom only ours"[685] and argues for a reconfiguration of the conceptualisation of privacy based on relationality.[686] Costello has explicitly argued for a relational privacy approach in Europe, though grounded in rights rather than the legislative regime.[687] Alongside these theoretical and normative works, there are many empirical and descriptive works of privacy and surveillance scholarship which demonstrate the interdependence of data sharing, particularly in light of social networking.[688]

In this chapter, rather than looking to alternatives to existing approaches to privacy and data protection, I seek to adopt a relational perspective to analyse our existing legal regime, particularly the GDPR and Article 8 of the Charter. In light of the centrality of the individual to EU data protection law, if we can accept that data interdependencies may exist in a variety of forms, it calls into question whether EU data protection law can respond to such forms of data.

If Nedelsky tells us a relational methodology can allow us to question the structures of relationships allowed by a regime, I approach EU data protection law in this light with two questions in mind. First, can EU data protection law accommodate relational data at all given its individual orientation? Second, what does the application of EU data protection law to relational data tell us about EU data protection law, including its conception of the individual and the structures of relationships it fosters?

---

[684] Including: Dean Cocking, 'Plural Selves and Relational Identity: Intimacy and Privacy Online' in Jeroen van den Hoven and John Weckert (eds), *Information Technology and Moral Philosophy* (Cambridge University Press 2001) <https://www.cambridge.org/core/product/identifier/CBO9780511498725A014/type/book_part> accessed 7 May 2020; Karen Levy, 'Relational Big Data' (2013) 66 Stanford Law Review Online 73; Sara Bannerman, 'Relational Privacy and the Networked Governance of the Self' (2019) 22 Information, Communication & Society 2187; Neil Richards and Woodrow Hartzog, 'A Relational Turn for Data Protection?' (2020) 4 European Data Protection Law Review 1; Laurent Sacharoff, 'The Relational Nature of Privacy' (2012) 16 Lewis & Clark Law Review 1249; Viljoen (n 48).

[685] Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78) 164.

[686] ibid 173.

[687] Costello (n 58).

[688] Including, Kurt Thomas, Chris Grier and David M Nicol, 'UnFriendly: Multi-Party Privacy Risks in Social Networks' in Mikhail J Atallah and Nicholas J Hopper (eds), *Privacy Enhancing Technologies*, vol 6205 (Springer Berlin Heidelberg 2010) <http://link.springer.com/10.1007/978-3-642-14527-8_14> accessed 23 September 2021; Gordon Hull, Heather Richter Lipford and Celine Latulipe, 'Contextual Gaps: Privacy Issues on Facebook' (2011) 13 Ethics and Information Technology 289; Gergely Biczók and Pern Hui Chia, 'Interdependent Privacy: Let Me Share Your Data' in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security*, vol 7859 (Springer Berlin Heidelberg 2013) <http://link.springer.com/10.1007/978-3-642-39884-1_29> accessed 23 September 2021; Iraklis Symeonidis and others, 'Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence' in Jaap-Henk Hoepman and Stefan Katzenbeisser (eds), *ICT Systems Security and Privacy Protection*, vol 471 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-33630-5_14> accessed 23 September 2021; Alberto Hermida and Víctor Hernández-Santaolalla, 'Horizontal Surveillance, Mobile Communication and Social Networking Sites. The Lack of Privacy in Young People's Daily Lives' (2020) 33 Communication & Society 139.

1.3. Relationality and plural personal data

One might approach relationality under EU data protection law in multiple ways and indeed there are existing important works which focus on the relationships between data subjects and data controllers[689] and between data processors and data controllers.[690] My starting point, grounded in Nedelsky's relational model, is that human beings are fundamentally relational, and considers the fundamental goal of EU data protection law: to protect the individual's right to data protection. Therefore, rather than focussing on the relationships which are explicitly created or recognised by the law, my approach is to consider how data protection may apply to relational data subjects.

As a proxy for relational data subjects, this chapter introduces the concept of plural personal data, drawing on the descriptive and empirical works of privacy and surveillance studies which describe scenarios in which multiple persons' data is captured simultaneously. This conception is founded upon the idea of the pluralism of the underlying data subjects, which intends to evoke the multiplicity and diversity[691] of the data subjects who may be captured by such a dataset.

A focus on the plurality of data subjects captured is in deliberate contrast to existing literature which focuses on group or collective data,[692] which we might think of as generally conceptualising the group or collective primarily in aggregation or as a corporate entity.[693] Relational approaches to the individual do not discount the placing of value upon the individual in contrast to those which root such value in the collective. As Nedelsky explains in her work on the relational self, "To say that relationships are fundamental to who and how human beings are is not to say that the collective powers (of government or community) that shape those relationships should take primacy over individual values."[694] Rather than group conceptions which often take for granted shared identities or interest, by focusing on the plurality of identities, we start from a point of diverse individual identities, and thus multiple diverse interests which may make up the many persons captured in the same dataset. In light of such diversity, we therefore must grapple with differences in preferences of individual data subjects and differential impact of data processing upon such data subjects.[695] Moreover, when EU data protection law is largely oriented around individual protection, a focus upon the relationality of individuals can be a fruitful means of examining whether human interconnection and interdependence be accommodated within the existing regime, rather than designing new approaches founded on collectivist approaches.

---

689 Matzner and others (n 310). A number of works consider the position of the child data subject, including Sheila Donovan, '"Sharenting": The Forgotten Children of the GDPR' (2020) 4 Peace Human Rights Governance 35.

690 Van Alsenoy (n 302).

691 George Crowder, 'Pluralism' in Mark Bevir, *Encyclopedia of Political Theory* (SAGE Publications, Inc 2010) <http://sk.sagepub.com/reference/politicaltheory/n347.xml> accessed 10 September 2020.

692 Edward J Bloustein, 'Group Privacy: The Right to Huddle' (1977) 8 Rutgers Camden Law Journal 218; David Mason and Charles D Raab, 'Privacy, Surveillance, Trust and Regulation: Individual and Collective Dilemmas of Online Privacy Protection' (2002) 5 Information, Communication & Society 379; Floridi, 'Open Data, Data Protection, and Group Privacy' (n 340); Mantelero (n 98); Floridi, 'Group Privacy: A Defence and an Interpretation' (n 98); Pagallo (n 98).

693 See e.g. Peter Jones, 'Human Rights, Group Rights, and Peoples' Rights' (1999) 21 Human Rights Quarterly 80.

694 Nedelsky (n 682) 33.

695 This conception of plurality takes some inspiration from Elinor Ostrom's observation that '[t]he world contains multiple types of individuals, some more willing than others to initiate reciprocity to achieve the benefits of collective action.' Elinor Ostrom, 'Collective Action and the Evolution of Social Norms' (2000) 14 Journal of Economic Perspectives 137, 138.

This concept of plural personal data anchors my analysis of relationality under EU data protection law. The GDPR and associated case law is reviewed, in order to examine the degree to which the regime recognises plural personal data, and thus whether a relational understanding of the individual is compatible with EU data protection law. Then, the implications of plural personal data on the functioning of the regime are considered, specifically, whether such data is subject to the GDPR in light of the requirement of "identifiability", the assessment of the legality of processing of plural personal data, the exercise of individual rights over plural personal data and whether the collectively-oriented elements of EU data protection law can accommodate plural personal data. In light of the implications of the regime for plural personal data, I reflect upon the conception of the individual under EU data protection law and the types of relationships and structures to which it contributes.

2. Plural personal data

As boyd has recognised, "Our data—and with it, our privacy—is increasingly networked."[696] There is an increased awareness of the ways in which data may relate to multiple individuals,[697] and increasing attention on theories of relational privacy.[698] This chapter suggests the term "plural personal data" to describe the phenomenon where data relates to more than one individual.

I suggest a distinction between two types of plural personal data; inherently plural personal data and developed plural personal data. This distinction is not the only possible organisation for mixed datasets, but this chapter uses the distinction due to the differences in both principle and application that arise for these different categories.

2.1. Inherently plural personal data

Some data inherently relates to multiple persons, because by its nature it reflects or records social or interrelated phenomena. We might point to genetic data, social data (such as photographs of multiple persons, communications data or social graphs[699]) as such types of inherently plural personal data. Data gathered about environments which individuals share (such as by smart devices installed in homes or work environments, or smart city projects) may also gather information which relates to multiple persons. In these cases, the data inherently relates to multiple persons due to what Barocas and Levy call a "tie-based-dependency"; the data captures the social or biological relationships between people,[700] or as I suggest, an environmental relationship.

Social interactions are often founded on sharing information with others, and are key to social experience and integral to forming and maintaining relationships. The emergence of

---

[696] danah boyd, 'Networked Privacy' (2012) 10 Surveillance & Society 348, 348.

[697] See e.g. boyd (n 696); Biczók and Chia (n 688); Karen Levy, 'Intimate Surveillance' (2015) 51 Idaho Law Review 679; Solon Barocas and Karen Levy, 'Privacy Dependencies' (2020) 95 Washington Law Review 555; Levy, 'Relational Big Data' (n 684); Bannerman (n 684); Nick Couldry and Ulises A Mejias, *The Costs of Connection : How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019); Karen Levy and Bruce Schneier, 'Privacy Threats in Intimate Relationships' (2020) 6 Journal of Cybersecurity 1.

[698] Richards and Hartzog (n 684); Urbano Reviglio and Rogers Alunge, '"I Am Datafied Because We Are Datafied": An Ubuntu Perspective on (Relational) Privacy' (2020) 33 Philosophy & Technology 595; Viljoen (n 48); Costello (n 58).

[699] A social graph is a generated map of interconnected relationships between individuals. Sangeet Paul Choudary, 'The Rise of Social Graphs for Businesses' [2015] *Harvard Business Review* <https://hbr.org/2015/02/the-rise-of-social-graphs-for-businesses> accessed 21 March 2019.

[700] Barocas and Levy (n 697) 4.

electronic communication and social networking services has led to the datafication of such information sharing and of the social ties between contacts. As Van Dijck points out, data-driven organisations have been very successful in convincing people to move many of their social interactions to online (and proprietary) environments.[701] Couldry and Mejias refer to this as social quantification.[702] As platforms record and capture communications between people, the resulting recorded and captured data is inherently plural personal data.[703]

A re-location of social interactions from an analogue to digital context, alongside facilitating the datafication of a range of social experiences, has also created and incentivised new forms of interaction which are now recorded in the form of plural personal data. Individuals may now use digital tools to track or keep tabs on others, named "lateral surveillance" by Andrejevic.[704] A variety of scholars have explored this phenomenon, adopting assorted labels, including 'horizontal surveillance'[705] and 'participatory surveillance'.[706] Whatever term adopted, each recognises a new form of interaction possible as every would-be sleuth is provided with a range of tools for monitoring others, and such monitoring is normalised and in some cases incentivised[707] or gamified.[708] The act of digital sleuthing itself generates another new form of social data is recorded, as the sleuth's investigations leaves a trail of digital breadcrumbs behind them in the form of search histories and metadata.

In the context of intimate relationships, this lateral surveillance has received particular attention. Levy has documented the variety of means for intimate partners to surveil their

---

[701] Van Dijck (n 30).

[702] Couldry and Mejias (n 697) 118.

[703] On the interdependence of data captured in association with social networking, see e.g. Anders Albrechtslund, 'Online Social Networking as Participatory Surveillance' (2008) 13 First Monday <https://firstmonday.org/article/view/2142/1949> accessed 7 May 2020; Thomas, Grier and Nicol (n 688); Hull, Lipford and Latulipe (n 688); Biczók and Chia (n 688); Symeonidis and others (n 688).

[704] Andrejevic points to background screening (e.g. looking up a date online before meeting), activity monitoring (e.g. tracking whether your emails have been read by recipients, tracking one's partner's online activities) and applications which purport to measure biometric signals to test truthfulness. Mark Andrejevic, 'The Work of Watching One Another: Lateral Surveillance, Risk, and Governance' (2002) 2 Surveillance & Society 488 <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3359> accessed 13 February 2020.

[705] Hermida and Hernández-Santaolalla (n 688).

[706] Albrechtslund (n 703). See also Kirstie Ball, MariaLaura Di Domenico and Daniel Nunan, 'Big Data Surveillance and the Body-Subject' (2016) 22 Body & Society 58.

[707] The use of behavioural psychological or economic theories have been adopted in the design of many digital environments, particularly digital marketing, often to seek to shape the engagement of users. Many data scholars have expressed concerns about such exploitation or manipulation. See, for example, Anthony Nadler and Lee McGuigan, 'An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing' (2018) 35 Critical Studies in Media Communication 151; Oscar H Gandy and Selena Nemorin, 'Toward a Political Economy of Nudge: Smart City Variations' (2019) 22 Information, Communication & Society 2112; Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review <https://policyreview.info/node/1410> accessed 10 September 2020.

[708] There is a range of literature on the gamification of online content, which seeks to elicit more user participation through the emulation of gaming with incentives and rewards. See, for example, David Easley and Arpita Ghosh, 'Incentives, Gamification, and Game Theory: An Economic Approach to Badge Design' (2016) 4 ACM Transactions on Economics and Computation 1; Juho Hamari, Lobna Hassan and Antonio Dias, 'Gamification, Quantified-Self or Social Networking? Matching Users' Goals with Motivational Technology' (2018) 28 User Modeling and User-Adapted Interaction 35; Jonna Koivisto and Juho Hamari, 'The Rise of Motivational Information Systems: A Review of Gamification Research' (2019) 45 International Journal of Information Management 191.

partners using digital technologies.[709] Danaher et al, building on Lupton's work on the quantified self[710] have pointed that a penchant for self-tracking and monitoring can extend to the monitoring and tracking of one's intimate relationships.[711] They suggest that there is no blanket objection to such monitoring.[712] Levy and Schneier on the other hand suggest that there are a number of privacy threats associated with intimate relationships, which hold potential for coercion and abuse.[713] Leaving the normative questions associated with intimate surveillance aside, it is a useful illustration of the potential for new forms of digitally mediated social interaction to simultaneously facilitate a new form of interaction and capture the data which records that interaction as plural personal data.

Other types of new data collection, provide for the datafication of social contexts where before the interactions and persons in those contexts would have been undocumented. We see this when sensors are embedded in a particular environment, leading to the capture of plural personal data relating to the persons who share that environment.[714] For example, a smart meter installed in a home may capture data relating to each of the inhabitants of that home, in relation to their common and independent activities. Moves towards "smart" cities can lead to the capture of data relating to entire populations.

Alongside social data, data which is inherently plural due to biological relationships has also taken on new significance in the context of increased capture and recording of genetic and health data.[715] Advances which have allowed for cheaper and quicker genome mapping have allowed for the generation and collection of new forms of biological data. But, as Panagiotopolos writes, genetic data has both communal and relational dimensions due to its shared nature.[716] Consumer genetic testing, ancestry mapping and DNA sequencing services all involve the collection of inherently plural personal data, given the ability to infer information about relatives from the data of another.[717] The popularity of such services has

---

[709] Levy, 'Intimate Surveillance' (n 697); Karen Levy, 'The Phallus-y Fallacy: On Unsexy Intimate Tracking' (2018) 18 The American Journal of Bioethics 22.

[710] Lupton has recognised how humans have become nodes for the generation and exchange of information, with the emergence of self-tracking and monitoring practices. Deborah Lupton, 'The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance' (2016) 45 Economy and Society 101.

[711] John Danaher, Sven Nyholm and Brian D Earp, 'The Quantified Relationship' (2018) 18 The American Journal of Bioethics 3.

[712] ibid 17.

[713] Levy and Schneier (n 697).

[714] See Meg Leta Jones, 'Privacy without Screens & the Internet of Other People's Things' [2015] Idaho Law Review 1. On the "Internet of Things" and the GDPR more generally, see also Nora Ní Loideáin, 'A Port in the Data-Sharing Storm: The GDPR and the Internet of Things' (2019) 4 Journal of Cyber Policy 178.

[715] Bygrave has noted this potential collective dimension of use of genetic and biological information, and the potential for a challenge in the application of data protection laws to account for group interests. Lee A Bygrave, 'The Body as Data? Biobank Regulation via the "Back Door" of Data Protection Law' (2010) 2 Law, Innovation and Technology 1. See also, for example, Paul Quinn and Liam Quinn's discussion of the new possibilities in medical research associated with 'big genetic data'. Paul Quinn and Liam Quinn, 'Big Genetic Data and Its Big Data Protection Challenges' (2018) 34 Computer Law & Security Review 1000.

[716] Adam Panagiotopoulos, 'Genetic Information and Communities: A Triumph of Communitarianism over the Right to Data Protection under the GDPR?' (2018) 4 European Data Protection Law Review 459, 460.

[717] Scudder et al have described the new possibilities of police investigations associated with familial searching on such databases. Nathan Scudder and others, 'Policy and Regulatory Implications of the New Frontier of Forensic Genomics: Direct-to-Consumer Genetic Data and Genealogy Records' (2019) 31 Current Issues in Criminal Justice 194. One high profile example saw the solving of a cold

led to some researchers estimating that approximately 60% of US individuals of European descent have a match of a third cousin or closer in genomic databases.[718] The relational nature of such data is relatively clear cut when it records a genetic relationship (e.g. ancestry and familial relationships captured), though the question of whether genetic information about one's immediate biological relations is data which inherently relates to oneself is less clear cut, though within the broad understanding of personal data, I suggest, possible.[719]

Therefore, there are certain datasets which, by the nature of the phenomenon which they seek to quantify and record, inherently relate to multiple persons. Inherently plural personal data offers us an avenue to think about the interpersonal and environmental relationships which shape individuals, and how pushes towards datafication of social lives, relationships and shared environments might impact the framing of data protection in terms of individual interests and rights.

2.2. Developed plural personal data

Alongside inherently plural personal data, there are certain types of data which relate to multiple persons, not because the data must be recorded in such a fashion due to its nature, but because the dataset has been so organised or created in order to perform certain data analytics or processing.

In order to leverage the possibilities of big data,[720] data is collected in massive databases which necessarily capture the information of many persons. Additionally or alternatively, new types of data capture are possible, through the digitisation and associated datafication of many arenas of life. Thus, while the data may not inherently relate to multiple people, it is rendered so by collecting it into a particular dataset, so that it may be analysed in a particular way. This may be in order to generate predictive insights for the purpose of sales or marketing, to generate databases of populations for the purpose of state surveillance, or to conduct research (both commercial and non-commercial).

Plural personal datasets may be developed in order to generate statistical insights about individuals in some instances. Many forms of modern data analytic modelling approaches are based on inferring individual behaviour based on models of groups or populations.[721] As

---

case murder case through such means. Zoë Corbyn, 'How Taking a Home Genetics Test Could Help Catch a Murderer' *The Observer* (1 December 2018) <https://www.theguardian.com/science/2018/dec/01/how-home-dna-tests-are-solving-cold-cases-golden-state-killer> accessed 21 March 2019.

[718] Yaniv Erlich and others, 'Identity Inference of Genomic Data Using Long-Range Familial Searches' (2018) 362 Science 690.

[719] Take for example a piece of data which records the fact that "Ann Smith" is a carrier of the BRCA1 gene which can cause a predisposition to certain types of cancer. This also has implications for "Mary Smith", Ann's daughter, as this data also carries the inference that Ann has a 50% chance of carrying this gene. It is at least arguable that therefore this data "relates to" both Ann and Mary, certainly in combination with other information, in the sense of *Breyer.* C-582/14 *Breyer* (ECLI:EU:C:2016:779)

Further, Kuru and Beriain make a normative case for genetic data to be considered the personal data of their identifiable relatives. Kuru and Beriain (n 58).

[720] Big data may be said to refer to "things one can do at a large scale that cannot be done at a smaller scale." Mayer-Schönberger and Cukier (n 30) 6. While there should be a healthy skepticism, or as Mireille Hildebrandt puts it "constructive distrust" in the "objectivity, reliability and relevance" of big data derived insights, the belief in the possibility of big data has been a powerful incentive for collection of data at scale. Hildebrandt (n 31) 36.

[721] Though there is debate as to whether the inferences derived from the population dataset fall within the definition of personal data, the better view seems to be that such inferred or derived data should be regarded as personal data. Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable

Marx explains, such surveillance is premised on an inference "going from group characteristics based on past events to future predictions about a given individual."[722] In order to generate a profile about a given individual, first a population must be documented and analysed. As a result, as boyd has observed, “Our interpreted selves aren’t simply the product of our actions and tastes; they’re constructed by recognizing similar patterns across millions of people. How machines see us depends on how our data connects to others”.[723]

However, these datasets are not always assembled or used with individual targeting in mind. When datasets are created and analysed at group or population level, a type of surveillance may be conducted which does not target at an individual level, but more broadly. For this reason, some have pointed to limitations in a individualist framing over broader big data surveillance,[724] and new collective mechanisms for data management in such framings have begun to emerge.[725] Indeed, cultivation of large datasets at population level, even if segmented according to certain types of activity, can be thought of as a new form of mass surveillance.

In both cases, whether individual or collective targeting is the aim, connections are drawn between notionally similar persons or groups of persons to classify and target subjects, and often to generate “predictive” insights about these persons. New revelations about individuals and collectives may be created, and new relationships between persons may be identified, based on insights as to types of discovered commonalities. Thus, we can say that data is gathered and new data created, which can be individual, collective and relational.

2.3. Accounting for plural personal data

If we accept that plural personal data may exist in a variety of forms, whether inherently plural or developed, it allows us to interrogate two issues. First, we can use the concept of plural personal data as a proxy for types of relationality (inherent due to interpersonal tie, or developed because of perceived correlations—such as situational or identity tie—which is being targeted for analytical purposes). We can use this proxy to examine whether EU data protection law can accommodate a relational understanding of the individual.

Second, we will see in this examination of how EU data protection law responds to plural personal data, how the law’s design/framing is premised upon an understanding of the person as primarily individuated, that is largely separate from other persons, and the implications of such a framing upon the operation of data protection law.

Finally, while it may be artificial to draw a bright dividing line between inherently plural personal data, and developed personal data, these categories offer useful points of analytical difference and commonality. Often in existing data protection literature, these types of personal data are categorised as creating different issues – inherently plural

---

Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI’ (2018) 1 Columbia Business Law Review 22–28 <https://osf.io/mu2kf> accessed 3 May 2019.

[722] Gary T Marx, ‘Coming to Terms: The Kaleidoscope of Privacy and Surveillance’, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 44.

[723] boyd (n 696) 349.

[724] For example, Cohen, ‘Studying Law Studying Surveillance’ (n 602); Mai (n 30); Kenneth A Bamberger and Ariel Evan Mayse, ‘Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age’ (2021) 36 Journal of Law and Religion 495.

[725] For example, data trusts or data commons. Sylvie Delacroix and Neil D Lawrence, ‘Bottom-up Data Trusts: Disturbing the “One Size Fits All” Approach to Data Governance’ [2019] International Data Privacy Law ipz014; Janis Wong, Tristan Henderson and Kirstie Ball, ‘Data Protection for the Common Good: Developing a Framework for a Data Protection-Focused Data Commons’ (2022) 4 Data & Policy e3.

personal data has received some attention in respect of relationality, sociality or interdependence.[726] Developed personal data has alternately been conceptualised primarily in terms of applying individually oriented laws at scale, associated with the "big data" phenomenon.[727] I argue in this chapter that there are commonalities as well as differences between inherently and developed personal data and their implications for data protection law. In common, both inherently and developed plural personal data may be said to raise questions about EU data protection law's efficacy, objectives or reach because of a mismatch between assumptions about personhood, the locus at which harms may occur, and the social environment in which the law applies. However, differences arise in the nature of the challenge and possible responses to those challenges. At the collection or creation phase, inherently plural personal data may be more difficult to legally resist, given that it captures something inherently relational about its subjects. Thus its very datafication needs to be challenged in order to resist the gathering of the data. Developed plural personal data, on the other hand, may be questioned at the point where its subjects' personal data is combined. The underlying normative considerations as to the desirability of the creation of such data is also somewhat distinct. Inherently plural personal data invites scrutiny of the mechanisms for the balancing of interests within EU data protection law, particularly in assessing when inherently plural personal data may be lawfully processed. Broader societal concerns as to the ends of the gathering of mass databases, and potential consequences at individual, group and societal level are relevant to the assessment of developed plural personal data.

3. Recognising plural personal data

As a first stage to considering whether EU data protection law's conception of the individual can accommodate relationality, we can look to whether the law expressly or implicitly recognises the existence of plural personal data. An examination of the GDPR, Article 8 and related guidance and CJEU decisions reveals three aspects of the law which address, at least partially, plural personal data. In considering (i) the definition of personal data, (ii) the data subject rights and (iii) the data controller obligations, a partial recognition of plural personal data arises.

3.1. Defining personal data and plural personal data

Personal data has particular meaning, and is a threshold concept of the GDPR and Article 8, integral to the definition of the material scope of EU data protection. Only personal data is captured by the GDPR.[728] Similarly, Article 8 extends the right to data protection by reference to such data, providing that "Everyone has the right to the protection of personal data concerning him or her."[729] Given the place of this threshold concept as determining the application of the GDPR, in order for plural personal data to be captured and regulated by the GDPR, it must first be considered to be "personal data".

An initial textual examination reveals that personal data as defined is framed in terms of a single person—the data subject—and each element of the definition is expressed in relation to that singular person. Article 4(1) of the GDPR defines personal data as

---

[726] Costello (n 58); Kuru and Beriain (n 58).
[727] van der Sloot, *Privacy as Virtue* (n 60); Manon Oostveen, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 International Data Privacy Law 299. See also Mittelstadt (n 340); Taylor, Floridi and van der Sloot (n 98).
[728] The GDPR applies "to the processing of personal data wholly or partly by automated means." Article 2(1), GDPR.
[729] Article 16 TFEU protects the right to data protection on the same terms.

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

This link to a single individual also has legal significance, in particular through the requirements that the information in question is "relating to" a data subject, and that a given data subject is "identified or identifiable". These two key aspects of the GDPR's definition of personal data have been given further meaning by the CJEU.

The question of when information "relates to" a data subject has been given a very broad interpretation. In *Nowak v Data Protection Commissioner,* the CJEU considered whether examination scripts and the comments by the correcting examiner were personal data which related to the examination candidate.[730] The CJEU determined that information relates to a data subject "where the information, by reason of its content, purpose or effect, is linked to a particular person."[731] This built upon the guidelines of the Article 29 Working Party,[732] and takes a broader approach than the earlier *YS* case.[733] Again, we can see that there is an emphasis on a singular person; a *particular* person. At the same time, the nature of the test is extremely broad,[734] and that breadth also renders it more likely that information might relate to more than one individual.[735] Interestingly, the Charter does not adopt this language of "relating to", but similarly reflects an individual protective approach, referring to personal data "concerning" the individual.

Similarly, determining whether information relates to an "identifiable" or "identified" natural person is also premised on an understanding of a singular person. We can see this from Recital 26 of the GDPR, which provides:

> *To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*

---

730 C-434/16 *Nowak* (ECLI:EU:C:2017:994).

731 ibid par 34.

732 The Working Party stated that "in order to consider that the data "relate" to an individual, a "**content**" element OR a "**purpose**" element OR a "**result**" element should be present." 'Opinion 4/2007 on the Concept of Personal Data' (Article 29 Working Party 2007) 01248/07/EN WP 136 10 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

733 Joined cases C-141/12 and C-372/12 *YS and Others* (ECLI:EU:C:2014:2081). The status of YS is somewhat unclear, particularly as the CJEU cited it "a contrario" to support its *Nowak* formulation. (Wong (n 217) 526. Lynskey, 'Criminal Justice Profiling and EU Data Protection Law' (n 192). Bygrave and Tosoni (n 217) 110.) The *Nowak* approach seems in principle a more coherent approach; separating the application of the regime from the purpose for which an individual seeks to exercise their right of access.

734 Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 86); Dalla Corte (n 86); Bygrave and Tosoni (n 217) 113. See discussion in Chapter 2, section 3.2(a).

735 The CJEU expressly acknowledges this, holding that "[t]he finding that the comments of the examiner with respect to the answers submitted by the candidate at the examination constitute information which, by reason of its content, purpose or effect, is linked to that candidate is not called into question by the fact that those comments also constitute information relating to the examiner." C-434/16 *Nowak* (ECLI:EU:C:2017:994), para 44.

As this Recital suggests, whether or not a given individual is identifiable can involve an extensive contextual examination, in particular for those cases where a person may be indirectly identifiable rather than directly. I return to this concern and its application to plural personal data in section 4.1 below.

While the definitional language of the GDPR and the functional application of the "personal data" elements might suggest an assumption that personal data is individually oriented, interestingly, there has been one acknowledgement of the possibility of plural personal data by the CJEU. In *Nowak*, the CJEU explicitly recognised that the same piece of data might be personal data in respect of multiple persons. Considering whether the applicant was entitled to access the comments of an examiner on the applicant's examination script, the Court determined that those comments were personal data relating the applicant, even though those comments also constituted information relating to the examiner.[736] While it is not explicit on the facts whether the examiner was identifiable (e.g. to the examining accountancy body), and thus whether it was also personal data relating to the examiner, it seems a fair assumption. Therefore, the CJEU has in principle recognised that the same piece of information might be the personal data of multiple persons. Interestingly, Advocate General Kokott went further, expressly stating that "the corrections made by the examiner are, at the same time, his personal data."[737]

Moreover, in some of the case law considering communications data, as Costello has observed, there is some recognition of the social nature of such data.[738] These cases do not arise under the GDPR/Data Protection Directive, but the ePrivacy Directive and Data Retention Directive, and so they were not concerned with the legislative definition of personal data, but nevertheless are instructive on the Court's approach to protected data under Articles 7 and 8. In *Digital Rights Ireland,* considering retained communications data by providers of public communications networks or publicly available electronic communications services, the Court observed that the data could allow "very precise conclusions to be drawn concerning the private life of the persons whose data has been retained", including "the social relationships of those persons and the social environments frequented by them."[739] Such data is said to fall within the meaning of personal data under Article 8, "because it constitutes the processing of personal data within the meaning of that article."[740] The same observation was reiterated about the communications data retained in the *Tele2, La Quadrature du Net, Commissioner of An Garda Siochána* cases.[741] Although not expressly considered, implicit in the recognition that communications data might capture

---

[736] C-434/16 *Nowak* (ECLI:EU:C:2017:994), para 44. "The finding that the comments of the examiner with respect to the answers submitted by the candidate at the examination constitute information which, by reason of its content, purpose or effect, is linked to that candidate is not called into question by the fact that those comments also constitute information relating to the examiner."

[737] C-434/16 *Nowak v Data Protection Commissioner* Opinion of Advocate General Kokott 20 July 2017 (ECLI:EU:C:2017:582), para 65.

[738] Costello (n 58) 17.

[739] Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238), para 27.

[740] ibid, para 29.

[741] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970), para 99; C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791), para 117; Case C-140/20, Commissioner of an Garda Síochána and Others (ECLI:EU:C:2022:258), para 45. These cases highlight a judicial awareness of the potential for greater harm associated with the aggregation of communications data across massive databases, see e.g. Nora Ní Loideáin, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 200.

social lives and relationships is the possibility that certain data sets may be the personal data of more than one affected individual: plural personal data. The recent decision of *OT v Vyriausioji tarnybinės etikos komisija* also contains such an implicit recognition, where the data on a public register might include information relating to the declarant's spouse or partner.[742] The CJEU made its assessment of the law requiring the data to be included on the public register by reference to the rights of the declarant under Article 7 and 8 of the Charter, but found that the publication of information which related to a specifically named partner or close relatives was deemed to go beyond what was strictly necessary in light of the objectives pursued.[743] The Court then expressly acknowledges that it is the personal data of both the declarant and any mentioned partners or relatives:

> *since it envisages such public disclosure of name-specific data relating to persons other than the declarant … the processing of personal data that is provided for in Article 10 of the Law on the reconciliation of interests also concerns persons who do not have that capacity and in respect of whom the objectives pursued by that law are not imperative in the same way as for the declarant.*[744]

Moreover, as Article 8 of the Charter should be interpreted as providing at least the same level of protection as offered by Article 8 of the ECHR,[745] it is worth noting that the case law of ECtHR illustrates some recognition of relational attitudes to private life and data protection. First, at a conceptual level the notion of private life under Article 8 of the ECHR has been framed as protecting, *inter alia,* "the right to establish and develop relationships with other human beings and the outside world".[746] Further, the ECtHR have recognised the relational nature of certain types of data, which are protected by Article 8 of the ECHR. It considered DNA profiles in *Gaughran v United Kingdom,* which were said to also impact biological relatives of the data subject.[747] Similarly, in *S and Marper v United Kingdom,* the ECtHR noted that cellular samples "contain a unique genetic code of great relevance to both the individual and his relatives."[748] Further, they noted that DNA profiles' "capacity to provide a means of identifying genetic relationships between individuals… is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned."[749] In *Odievre v France*, concerning the right of a child to know the identity of her biological mother,[750] the ECtHR noted that "[t]he expression "everyone" in Article 8 of the Convention applies to both the child and the mother."[751] Moreover, the ECtHR acknowledged a conflict between these two private interests, which also "cannot be dealt with in isolation from the issue of the protection of third parties" and a general interest of the protection of life safeguarded by the underlying legislation.[752] Beyond genetic relations, the

---

[742] C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601).
[743] ibid, para 96.
[744] ibid, para 100.
[745] See Chapter 2, section 2.2(a).
[746] *Perry v United Kingdom* App no 63737/00 (ECtHR, 17 July 2003), para 36. See also e.g. *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000), para 65; *PG and JH v United Kingdom* App no 44787/98 (ECtHR, 25 September 2001), para 56; *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 66; *Von Hannover v Germany (No. 2)* Apps nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), para 95; *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017), para 70.
[747] *Gaughran v United Kingdom* App no 45245/15 (ECtHR, 13 February 2020).
[748] *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 72.
[749] ibid, para 75.
[750] *Odievre v France* App no 42326/98 (ECtHR, 13 February 2003).
[751] ibid, para 44.
[752] ibid.

ECtHR has also recognised how other forms of social relations can engage Article 8 of the ECHR. In *Bărbulescu v Romania,* in the context of monitoring of employees, the ECtHR considered that restrictions on professional life fell within Article 8 "where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others."[753]

Thus, while the definitional language describing personal data in the GDPR is quite individually oriented, the CJEU has recognised the possibility of particular data being related to more than one individual, as have the ECtHR in the context of Article 8 of the ECHR. Thus, plural personal data may be "personal data" within the meaning of the GDPR and Article 8, provided it satisfies the usual criteria by reference to at least one of the captured data subjects.

3.2. Plural personal data and data subject rights

The second area in which we see some recognition of the potential for multiple data subjects to be captured in a given dataset is in the provisions providing for the data subject rights under the GDPR. These rights, individually exercisable, may be exercised over plural personal data, and the GDPR makes some provision to prevent the use of these rights to interfere with the interests of others, though the provisions are uneven across the data subject rights.

The clearest recognition and only apparent express recognition of multiple affected data subjects is seen in the provisions concerning the right to data portability. This right to port one's data from one data controller to another is subject to a caveat in Recital 68 of the GDPR, which notes that:

> *Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation.*

The Article 29 Working Party clarified that the provision that the right to data portability "shall not adversely affect the rights and freedoms of others,"[754] is "intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects."[755] The guidelines acknowledge the possibility of data sets containing the personal data of more than one person,[756] and in such a case, a new legal basis for the processing of that third party data must be found.[757] The guidelines consider bank account data and contact lists uploaded to an email service. Curiously the guidelines emphasise that such data may be processed by a service provider "only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs."[758] This suggests that the requesting user *qua* data subject exercises the right to data

---

[753] *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017), para 71.
[754] Article 20(4), GDPR.
[755] 'Guidelines on the Right to Data Portability' (Article 29 Working Party 2017) 16/EN WP 242 rev.01 11 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.
[756] "The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with that controller. Where personal data of third parties are included in the data set another legal basis for the processing must be identified." ibid.
[757] ibid.
[758] ibid 12.

portability (as this is a right which a data subject enjoys) requesting the data to be transferred from the original data controller to a secondary service provider. However, upon transfer the individual data subject must acquire new status as an empowered data controller and the receiving entity a data processor.

The possibility of plural personal data is also acknowledged in the provisions of the GDPR which deal with the right of access. Particularly, the GDPR provides that "[t]he right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."[759] However, it does not have an equivalent to Recital 68, expressly recognising mixed datasets, despite the same risk arising that the right might be exercised in relation to plural personal data. Rather, Recital 63, which does acknowledge potential impact on others, seems to have in mind the burden upon the disclosing controller, providing that:

> *That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.*

The inconsistency of approach across the various data subject rights is even clearer when we turn to the remaining rights. The rights to rectification, erasure, restriction of processing and to object do not have any equivalent provisions. Yet it appears just as clear that these rights might be exercised over plural personal data, and therefore the same risks of adverse impact on other affected individuals arise. What if I seek to exercise my right to erasure over plural personal data? Should my desire to erase the relevant content override my co-data subjects right to continued storage and processing of that data? The best guidance we can take from the GDPR, is that balancing of rights approaches have been adopted with regard to access and portability, and this might also be suitable for other clashes between affected data subjects. Without any express provisions or guidance on the area, controllers and data subjects alike are left with uncertainty due to an apparent lack of coherent thinking across the data rights. The implications of the individual exercise of these rights over plural personal data are considered in further depth in section 4.3 below.

3.3. Plural personal data and controller obligations

There is some recognition of the potential for plural personal data in the provisions of the GDPR concerning obligations of the data controller. Each of these provisions make reference to the many natural persons who are affected by the data controller's actions but, as we shall see, there is little indication of the nature of the plurality affected, nor any interdependence of the relevant persons.

The primary requirement of the data controller, to ensure data processing occurs in compliance with the requirements of the GDPR, requires the controller to take into account "the risks of varying likelihood and severity for the rights and freedoms of natural persons".[760] This language is then replicated across the obligation to implement data protection by design,[761] to have appropriate security measures in place,[762] the obligation to notify security breaches,[763] and to conduct a data protection impact assessment.[764] Some of the other provisions make reference to data subjects in the plural form, particularly the requirement to

[759] Article 15(4), GDPR.
[760] Article 24, GDPR.
[761] Article 25, GDPR.
[762] Article 32, GDPR.
[763] Articles 33-34, GDPR.
[764] Article 35, GDPR.

hold records (including descriptions of categories of data subjects),[765] to designate a data protection officer[766] and the possibility to prepare codes of conduct.[767]

Each of these provisions suggest a recognition of the potential for data controllers to affect data subjects (or indeed other natural persons) at scale. However, without any consideration for the interdependence of these interests such as seen in the right to data portability, the conception of a plurality of data subjects or persons in these provisions accords with a conception of aggregation of individual data subjects. While data processing at large scale triggers some additional bureaucratic obligations upon controllers,[768] the existence of these multiple data subjects does not otherwise alter the regulatory approach as compared to when a single data subject is concerned. This suggests that any idea of multiple affected individuals may simply be aggregated in their individual interests, without any regard to the interdependencies or diversity in interests which might be represented by such a plural dataset.[769]

3.4. Uneven recognition of plural personal data

In consequence, we can say that the recognition of plural personal data is partial at best. Plural personal data may be subject to the GDPR or protected by Article 8, but likely only insofar as it satisfies the usual definitional conditions of "personal data", and in *Nowak* and *OT* we see a recognition by the CJEU of the potential for plural personal data to be the personal data of more than one individual. The right to data portability is exceptional in its express consideration of how an individual might seek to exercise a right over data of multiple persons, and the data controller obligations suggest collectives of data subjects are mere aggregations of individual interests.

Despite the GDPR's acknowledgement of the role of data in contributing to social life,[770] this has not translated to consistent treatment of mixed datasets in the GDPR. Yet, when plural personal data can exist in many forms, this necessarily calls into question how the GDPR applies to such sets, when many of its provisions are individually-oriented. Further, insofar as collective approaches exist in the GDPR, I consider how an aggregation of isolated individual interests fails to account for the relational nature of plural personal data.

4. Accommodating plural personal data

Accepting that plural personal data exists in a variety of forms, and that the GDPR did not expressly provide for the treatment of such data except in very narrow circumstances, we might question whether EU data protection law can accommodate such data at all? The

---

[765] Article 30, GDPR.
[766] Article 37, GDPR.
[767] Article 40, GDPR.
[768] With certain categories of data, to conduct a data protection impact assessment (Article 35(3), GDPR), and to designate a data protection officer (Article 37, GDPR).
[769] A striking illustration of this idea is found in the decision of *OT v Vyriausioji tarnybinės etikos komisija,* wherein the Court considered the legality of a national provision which provided for the public disclosure of data regarding financial interests for anti-corruption purposes, which might contain the data of multiple parties. In considering the nature of potential harm associated with this data processing, the Court suggest an aggregative approach, finding that "[t]he seriousness of such an infringement may still be increased by the cumulative effect of the personal data that are published as in the main proceedings, since combining them enables a particularly detailed picture of the data subjects' private lives to be built up." Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601), para 101.
[770] Recital 6, GDPR. Further, Recital 85 accepts that a data breach may cause social disadvantage to an affected person.

section considers the implications of the existence of plural personal data on the manner in which data protection law functions, by reference to the role of the individual in the regime.

This section does not purport to be an exhaustive examination of these implications, but is particularly looking to three aspects of the regime; (i) the scope of the GDPR's application, (ii) how an assessment of the legality of data processing may proceed with regards to plural personal data, and (iii) how individual data rights and rights of action may be exercised with regards to plural personal data.

4.1. The limits of identifiability and plural personal data

The existence of plural personal data may call into question the apparent conflict between an individually defined material scope and plural personal datasets. After all, if such datasets exist, when are they captured by and therefore subject to EU data protection law? I argue that a difference appears between inherently plural and developed plural personal data. Moreover, this investigation illustrates the importance of identifiability as a normative anchor under the GDPR, which allows us to question the implicit assumptions which underly EU data protection law, including about the nature of the person to be protected.

Anonymised data is not subject to the GDPR or Article 8.[771] We might then ask, what is the distinction between a dataset wherein multiple persons are identifiable and therefore it is plural personal data (and subject to the law) and aggregated data? At what point do the data subjects drown one another out such that the individuals can no longer be distinguished from the crowd? When is a plural personal dataset anonymised?

The line to be drawn between personal data and anonymised data is that of identifiability,[772] and it would seem to be the same for plural personal data, at least under the current regime. Once there are identifiable individuals in the plural personal data, it will be subject to EU data protection law. The question therefore, is whether underlying persons are identifiable in plural personal data at the point at which it relates to them.

As a preliminary matter, we should note that there is no suggestion in the language of the GDPR that identifiability must be limited to a single individual in a given dataset. Further, that would run contrary to the CJEU's acknowledgements in *Nowak* and *OT* that the data of more than one data subject could be present in one piece of data. Indeed it would significantly undermine the protective effect upon individuals if simply the fact of multiple affected individuals took it outside the realm of data protection.

Recital 26 of the GDPR does refer to the "singling out" of an underlying data subject, though this is an illustration of a means of identifiability rather a criterion of it. The Recital provides, *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."* Bygrave and Tosoni point out that this reference to "singling out" originates from Article 29 Working Party guidance on the nature of identifiability under the Data Protection Directive, and is intended "to provide an elaboration of identifiability, not to add a new and separate criterion", and they conclude that

---

[771] Recital 26 of the GDPR provides: *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*

[772] ibid.

the result is not a substantial change to the approach to identifiability under the Data Protection Directive.[773]

The challenges of identifying underlying data subjects in plural personal datasets comes into focus when we contrast inherently plural and developed plural personal data. We remember that inherently plural personal data stems from the datafication of existing relationships (whether social, biological or otherwise). When the target of the data record or analysis are still individuals (though in an interconnected sense), identifying such underlying individuals should in principle be feasible. If we think of social data, the purpose is usually to communicate from one to another (or possibly multiple), necessitating identification. Familial or biological records similarly seek to record the underlying individuals' connections. Thus when it comes to inherently plural data, the threshold of identifiability will often be possible, and EU data protection law nominally applicable. The consequences of such application will be further considered below.

When it comes to developed plural personal data, challenges of identification become greater. When data is collected for larger scale processing purposes, it may not fit within the conventional identifiability paradigm. The target of the data analytics may not be at the individual level, but rather the insights to be generated may be at a group or population level (e.g. behaviours of groups of certain ages or in certain geographical areas).[774] For this reason, at the analysis stage, as Oostveen has written, the GDPR may not be applicable to big data sets.[775] However, as Oostveen points out, this is not to say that the GDPR may not be applicable at the point of data acquisition.[776] Indeed, the cases in which the CJEU has emphasised that mass and indiscriminate surveillance by states is unlawful by reference to the rights of data protection and respect for private life under the Charter illustrate that individualised rights-based approaches can be applied to prohibit the creation of mass databases.[777]

The requirement of identifiability highlights the normative role that individual identification plays in EU data protection law. Dalla Corte argues that data protection is intended to protect individuals, not the groups to which they belong, and therefore the "identifiability" of the underlying person plays a key delimiting role in determining the material scope of EU data protection law.[778] In other words, if there is no identification of an underlying individual, the argument goes that it is less likely that that individual impact or harm might occur as a result of the data processing. Dalla Corte suggests this illustrates the limits of the GDPR's ambition in tackling harms may lie.[779] I agree with Dalla Corte's analysis of the functional limitation of the identifiability criterion. However, rather than an explicit limitation in ambition, it might be better to consider this focus on individual harms as a product of historical and conventional

---

[773] Bygrave and Tosoni (n 217) 108–109.
[774] This is the same reason some scholars suggest that protection of the individual should be supplemented by looking to information which categorises or groups. Taylor, Floridi and van der Sloot (n 98) 5.
[775] Oostveen (n 727).
[776] ibid.
[777] See Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238); Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970); C-623/17 *Privacy International* (ECLI:EU:C:2020:790); C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791); Case C-140/20, *Commissioner of an Garda Síochána and Others* (ECLI:EU:C:2022:258).
[778] Dalla Corte (n 86) 10.
[779] ibid.

understandings of data protection and privacy harms in terms of the individual.[780] EU data protection law is founded on a logic of protection of the individual which we associate with liberal rights frameworks dating from the 18th and 19th centuries, and a corollary assumption that such rights regimes will effect individual protection.[781] Such rights frameworks have come under criticism for a variety of reasons by a range of scholars (feminists and relational theorists among them), including those who critique individual rights-based frameworks (particularly rights to privacy) as disregarding impact on issues of justice and equality, and the amassing of significant power by data controllers.[782] Central to many of these critiques is not simply a misplaced focus on individuals, but criticism of the way in which the individual is conventionally conceived in traditional approaches.

Thus, examining the normative role that identifiability plays in EU data protection law is useful for two purposes. First, as Dalla Corte suggests, it illustrates a functional limitation as the GDPR purports only to protect individuals and seeks to implement this limitation through the use of the identifiability criterion to limit its scope. Whether the GDPR even fulfils this ambition to protect individuals is challenged when relational data such as plural personal data exists, as will be explored in the following sections. Second, this function of the identifiability criterion reminds us that the law is founded upon a particular idea of personhood and individuality, and how data protection purports to apply is shaped by that idea. A limitation to individual protection may not be an explicit limitation in ambition but an implicit result of an understanding of the order of things and the function of law in relation to the person. When we re-engage with these implicit understandings, we are in a position to better question them.

4.2. The legality of processing plural personal data

Considering the general rules for the legality of the processing of personal data, we also see that plural personal data may cause challenges for the assessment of the legality of such data. In considering the processing of plural personal data, I focus on three aspects of the GDPR's regulation of data processing: (a) the legal basis for processing, and (b) the data protection principles, and (c) the enforcement of the GDPR.

(a) Legal basis for processing: individualised standards and plural personal data

As a pre-condition to data processing, the data controller must be able to justify their processing on one of six legal bases.[783] Three we might describe as individually-oriented, two have a public-orientation and the final legal basis is a hybrid, considering multiple parties. While the individualised nature of these standards has already been explored,[784] it is worth remembering that the final pre-condition to processing (necessity for a legitimate interest) offers us an illustration of an express recognition of multiply affected parties, and how the GDPR seeks to balance competing interests.[785] However, it is still premised upon

[780] See Chapter 3.
[781] ibid.
[782] E.g. Christian Fuchs, 'Towards an Alternative Concept of Privacy' (2011) 9 Journal of Information, Communication and Ethics in Society 220; Lindsay Weinberg, 'Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden' (2017) 12 Westminster Papers in Culture and Communication 5; Cohen, 'Turning Privacy Inside Out' (n 379).
[783] Article 6, GDPR.
[784] See Chapter 2, section 3.2.
[785] Article 6(1)(f), GDPR.

the impact on an individual data subject, whose interests or fundamental rights and freedoms must be weighed.[786]

Therefore, to the extent that the legal pre-conditions for processing draw upon an individualised assessment, we can generalise that it is because the pre-conditions are premised on an individual's acquiescence to the processing (either through consent or entering into an associated contract) or because the legal standard of review is based on consideration of the rights or interests of an individual.

If we are to consider the legal bases which are premised upon individual acquiescence to processing, plural personal data seems to create a particular challenge. After all, if one individual chooses to consent to processing or enter into a contract, and plural personal data (of which they are only one party) is processed, can such consent or contractual necessity justify the processing in respect of all such data? This gives rise to what may be described as a "privacy externality",[787] or as Barocas and Nissenbaum name it "The Tyranny of the Minority".[788] This tyranny manifests differently depending on whether we are considering inherently plural personal data or developed plural personal data. In inherently plural personal data, we can imagine that one individual may acquiesce to the processing of the personal data of others where the data is mixed. As explored in section 2 above, plural personal data may be generated through a variety of processing technologies, and thus whenever an individual, for example, uses communication or social networking services, buys a connected device or vehicle, has their DNA commercially tested, they may be volunteering their own data to be processed, and they may also be surrendering the data of their associates. Developed plural personal data may also involve such a tyranny, and indeed, it was in this context Barocas and Nissenbaum wrote. In cases of developed personal data, the voluntary data subject may not be expressly providing the data of others, but as Barocas and Nissenbaum write, there is the potential to infer data of the majority based on the volunteered data of a minority of willing few.[789] The GDPR does not make any express provision for how a difference in opinion could be mediated where one data subject wishes for the processing of their shared data and the other does not. However, in situations where the data controller has a legal basis for processing that data with respect to one data subject but not the other, in principle it puts them in a position that they are simultaneously lawfully and unlawfully processing the same piece of data.[790]

Those legal bases which are subject to assessment by reference to an individual's rights or interests are those which consider the vital interests of a data subject or of another natural person, or the public interest and legal obligation grounds. It would seem that such an individualised assessment might not compromise the treatment of plural personal data if we can assume that the data protection interests of the relevant data subjects are aligned, and

---

[786] Article 6(1)(f), GDPR provides: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." (My emphasis.)

[787] Simeon de Brouwer, 'Privacy Self-Management and the Issue of Privacy Externalities: Of Thwarted Expectations, and Harmful Exploitation' (2020) 9 Internet Policy Review <https://policyreview.info/articles/analysis/privacy-self-management-and-issue-privacy-externalities-thwarted-expectations-and> accessed 28 April 2021.

[788] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 61. See also a similar argument in Sætra (n 104).

[789] Barocas and Nissenbaum (n 788) 61.

[790] See further Chapter 5.

all subjects are comparably affected by the data processing in question. However, if the data subject complainant is not representative of all concerned data subjects, an individualised rights-based assessment risks a similar dilemma to the tyranny of the minority seen in cases of individual acquiescence to processing. Given the risk of disparate impact of a given processing operation depending on each person's individual circumstances,[791] if the legality is measured by reference to a particular archetypal data subject, there is danger of discriminatory impact. In particular, minorities, marginalised or disadvantaged persons may be unfairly impacted merely because their perspective is insufficiently similar to the average to have been weighted in the assessment of legality. With regard to inherently plural data, it may be feasible to actually identify and consider the positions of each data subject, but in cases of developed plural personal data, large scale datasets make this less possible, and a greater risk of discriminatory impact seems plausible (particularly if the dataset is being analysed to identify commonalities between groups rather than difference).

There is a provision of the GDPR which suggests recognition of differential impact of the harms of processing, but it does not seem to have been integrated more broadly into the legislative framework, and is rather framed as a matter for data controllers to consider. Recital 75 of the GDPR elucidates the risks that may be posed to individuals by data processing, noting that

> *The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage", and considers a number of forms that the damage could take (including discrimination, financial loss, revelation of special categories of data, amongst other forms).*[792]

We can see that the provision recognises that those risks may be of "varying likelihood and severity" which is open to being interpreted as a recognition of the differential impact that data processing may have on individuals. Equally, without further guidance, it may also be

---

[791] Michael McCahill and Rachel Finn have illustrated the differential impact of surveillance on different subjects. Michael McCahill and Rachel L Finn, *Surveillance, Capital and Resistance: Theorizing the Surveillance Subject* (Routledge 2015). The work of many critical race scholars and feminist scholars have illustrated the additional discriminatory burden that data processing practices can place on women, ethnic and racial minorities and marginalized persons. For example, Browne (n 522); Noble (n 522); Benjamin (n 522); Lauren F Klein and Catherine D'Ignazio, *Data Feminism* (MIT Press 2020).

[792] In full, Recital 75 provides: "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects*." Interestingly, as Eleni Kosta notes, these provisions refer to 'natural persons', rather than data subjects. Eleni Kosta, 'Article 35. Data Protection Impact Assessment' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 671.

interpreted to refer to a common impact which is dependent on the nature of the processing in question. However, even if this was a legislative recognition of such differential impact, it does not seem to have called into question the fact that individualising rights and practices can contribute to such discriminatory impact, and we can see the risk of this occurring in an individualised assessment of the legality of processing over data which concerns multiple persons.[793]

The legitimate interests ground gives us the best indication of how the GDPR purports to deal with differing interests between multiple parties; a balancing of the interests between the controller or a third party and the interests, rights and freedoms of the data subject. However, the analysis is premised upon a single data subject. Thus, an assessment of legality by reference to a single data subject in respect of plural personal data will only be effective protection for the entire dataset if the data subjects' interests and experiences are aligned.

In plural personal datasets, therefore, we can see that the legal bases for processing run the risk of failing to consider the interests of all those affected. The EU data protection framework seems to largely operate on the conception of an individually affected data subject, whose data may be segmented from the rest of the population. The requirement of identifiability operates to individuate affected persons, and data protection's individual data subject is largely not seen in a relational lens. I suggest the existence of plural personal data challenges this framework and conception of the individual. First, challenges may arise where preferences between data subjects in a plural personal dataset differ, and they wish to exercise conflicting choices over the data in question. Either a data subject's self-determinatory exercise of consent must be denied or their co-data subject's denial of consent must be disrespected. Second, a particular individual claimant, or an archetypal notional data subject, may come to represent others in a plural dataset in the assessment of the legality of the processing of that dataset. If there is consensus on the impact of that processing, this is not necessarily insurmountable, but there is a risk of injustice in the impact upon co-data subjects who are different in their experience of such processing.

(b) Data processing principles

Personal data must be processed in accordance with six data protection principles.[794] When we look to the data protection principles, we see that they are less explicitly tied to the data subject, as compared to the legal bases for processing.

Indeed, only two of the data protection principles are defined by reference to the data subject. First, the lawfulness, fairness and transparency requirement is assessed 'in relation to the data subject',[795] though the requirement of fairness in Article 8 is not so tied to the subject.[796] Second, the storage limitation principle requires that personal data is kept in a form which permits identification of data subjects no longer than is necessary for the purpose of processing.[797]

---

[793] The connection between individualised assessment and difference will be further explored in Chapter 6.
[794] Article 5, GDPR.
[795] Article 5(1)(a), GDPR.
[796] Article 8(2) provides (in part): "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*."
[797] Article 5(1)(e), GDPR.

On the other hand, the purpose limitation requirement, data minimisation, data accuracy and integrity and confidentiality principles are all expressed generally, without using the data subject as a focus of the principle.[798]

When we come to consider the substance, over the mere textual interpretation of the principles, we can see that given their focus on the data processing, that the majority are concerned with influencing the practices of processing, and are not focussed on individual data subjects but on the activities of the data controller. It is the lawfulness, fairness and transparency principle which relates most to an individual, as compliance with its terms will necessarily invoke the consideration of an affected individual data subject, though it has a broader benefit also in terms of regulating data controller conduct generally.

The principles provide for general principles of data governance, which might be said to formally benefit all data subjects. These principles ensure a basic set of standards with which data controllers must abide, and in setting such standards limit the data controller's freedom to impact persons. When the data subjects are similarly placed, they should all benefit; data minimisation, storage limitation, purpose limitation, transparency etc. should notionally ensure good data governance which benefits all the data subjects. These principles govern *how* a data controller may engage in processing.

By contrast, the individual data subject becomes the focus of the test of legality when we come to ask *why* that processing may occur (lawfulness, fairness and transparency). In the absence of any consensus on the permissible purposes to process personal data, when the GDPR comes to assess why processing may occur, then the assessment is once again somewhat individually oriented. The first data protection principle (lawfulness, fairness and transparency) measures the legality and fairness of such processing by reference to a given data subject.

This might lead us to question; how do we assess the impact on affected data subjects if the processing affects plural personal data? There is no guidance in the GDPR, and we return again to the challenges I introduced in regard to an individualised assessment of legality in section 4.2(a) above. If the processing is fair by reference to one data subject, but unfair by reference to another, and the processing of their data is indivisible, how is a data controller to proceed? This creates more challenges by reference to inherently plural personal data than developed personal data where the data of the respective data subjects may be divisible, but subject exclusion may undermine the efficacy or quality of big data analytics. It would seem, therefore, that while the data protection principles, insofar as they have a more collective or generalised orientation, are useful for the regulation of plural personal datasets where there are shared data protection interests (i.e. the interest in good general data governance). When, however, the interests, rights or preferences of the underlying individuals differ, we are once again challenged in the application of these principles to plural personal data, and the GDPR's understanding of the individuated data subject is once again apparent.

Alongside the six data protection principles, the GDPR added an additional principle, the accountability principle.[799] Its orientation is different to the rest of the principles, as rather than focussing on the substance of data processing, it is concerned with compliance with the GDPR. This principle stands for the data controller's responsibility for compliance and also its responsibility to be able to demonstrate that compliance. It is interesting for a number of

[798] Articles 5(1)(b), (c), (d) and (f), GDPR.
[799] Article 5(2), GDPR.

reasons, but in particular because it is our best illustration of how the GDPR envisages the application of its obligations at scale to multiple data subjects. A data controller is understood to potentially process the data of multiple data subjects (whether its many customers, employees, patients, students etc.) For many of its obligations, the data controller is bound to consider the potential risks to the rights and freedoms of affected persons,[800] and in these provisions we see an indication of how the GDPR envisages its operation at scale. The data controller's obligations are framed as potentially applying to many subjects, but the obligations are not prescribed per data subject but per data controller. Thus the governance measures that a data controller must adopt (security measures, transparency notices, data protection impact assessments and breach notifications) are not tailored per individual data subject, but are designed to applying to a mass of homogenous data subjects, an interesting contrast to the individuated emphasis seen in the previous principles.[801]

Thus when we come to consider the application of the data protection principles to plural personal data, we see an extension of the individuated understanding of the legal bases for processing. When there is a question as to *why* data may be processed, the individualised emphasis under the data protection principles mirrors that of the legal bases for processing: the test for legality is linked to either an individual's acquiescence or assessment of impact upon an individual's rights or freedoms. For plural personal datasets, this raises challenges when there is either a difference of preference or position. But beyond this, the data protection principles also offer us a reasonable basis for seeing how EU data protection law can provide common standards of data governance which might scale. In the cases of the requirements regarding security standards, breach notifications, transparency and data protection by design obligations, the EU legislature overrides any individual preference for lower protective standards, and sets a common standard of protection. In doing so, there is an implicit homogenisation of the underlying data subjects into a common class who will be similarly benefited from these protective standards. While not apparently designed with plural personal data in mind, in principle it can apply just as well to plural personal datasets as to aggregations of individual data subjects, but will be limited when the interests of the underlying individuals are not aligned, and particularly where discriminatory impact is felt by certain individuals.[802]

4.3. Enforcement

The procedural apparatus for the enforcement of EU data protection law provides for individually exercisable rights, representative actions and supervision by data protection authorities. In considering the utility of these provisions over plural personal data, we see a similar dynamic emerging as encountered in assessing the legality of processing plural personal data. Individually exercised rights can fail to respect the interests of co-data subjects, and betray an individuated understanding of the data subject. Representative actions and supervisory interventions can operate to protect plural personal datasets, but only in the same way that they are useful for aggregations of data subjects: where their interests are aligned.

---

[800] Recital 75, GDPR. See section 3.3 above.
[801] Though, at times the CJEU has prescribed that individual specific action may also be warranted. See discussion in Chapter 6, section 3.
[802] See further Chapter 6.

(a) Individually exercisable rights and plural personal data

The individual qua data subject enjoys a number of rights which they may exercise in order to safeguard their data and enforce the provisions of the GDPR; rights which may be exercised against data controllers and rights to certain judicial remedies. Clearly, the capacity to exercise such rights by an individual in respect of plural personal data raises some questions. Much like the legal pre-conditions to processing which are based on the exercise of a type of individual control (consent, contractual necessity), where individual decisions are made about the processing of plural personal data, there is the potential for disagreement.

Data subject rights which may be exercised against data controllers were introduced in section 3.2 above, where I argued that there is little recognition in the GDPR of the potential for the impact of an individually exercised right upon the data of others. The GDPR provides little basis for the mediation between competing interests of different data subjects in such cases beyond a suggestion towards rights balancing, at the same time it is clear in reference to other obligations that data controllers must consider the risks posed to all affected natural persons.[803] On a practical basis, it appears that many controllers address this matter in subject access requests by redacting data disclosed to subjects where third parties are identified.[804] While imperfect and potentially very costly for data controllers, at least such approaches allow for the exercise of individual requests over plural personal datasets to be achieved in a way which balances the interests of multiple parties. But other rights create greater challenges, as how to reach an accommodation between various parties is less obvious. While the regulatory guidance points to the role for individuals to take on the status of data controllers in places,[805] such an approach comes with its own challenges.[806]

Similarly, we can imagine the exercise of the rights to rectification, erasure, restriction or to object by one data subject could come into conflict with the preferences of other data subjects, who might have a different vision of whether, for example, data is accurate, or lawfully processed. The desire of one data subject to exercise his or her rights against a controller in respect of a plural personal dataset gives us a concrete example of the potential for data subjects interests to clash, and yet, the law does not provide guidance for the mediation between competing interests or preferences of different data subjects in such cases. The absence of such consideration points again to an understanding of an individuated, rather than relational individual informing the GDPR's framework and its conception of the data subject.

The pursuit of a judicial remedy by a data subject[807] may also impact other individuals; either because the processing of a plural personal dataset changes, or because while their data is not plural personal data it may be similarly processed by the same data controller. An action by an individual may have positive effects for other data subjects, if one person highlights

---

[803] Recital 75, Articles 24(1), 25, 32-35 GDPR.

[804] The Information Commissioner's Office have released detailed guidance on appropriate responses to redaction. 'How to Disclose Information Safely: Removing Personal Data from Information Requests and Datasets' (Information Commissioner's Office 2018) <https://ico.org.uk/media/2013958/how-to-disclose-information-safely.pdf>.

[805] With respect to the right to portability, see section 3.2 above.

[806] See Natali Helberger and Joris van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers' (2010) 11 Computer Law Review International 101; Edwards and others (n 83); Mahieu, van Hoboken and Asghari (n 387). Further, discussion in Chapter 2, section 5.3.

[807] The right to complain to a data protection authority (Article 77, GDPR), to an effective judicial remedy against a data protection authority or a controller or processer (Articles 78 and 79, GDPR.)

illegal processing and this results in the cessation of such illegal conduct, then all affected data subjects will benefit. However, the particular data subject in question, and their experience of the data processing in question may come to be determinative as they come to represent their co-data subjects. Again, if the assessment of legality which occurs is framed in terms of their position, it risks under-protecting co-data subjects who are differently positioned.

(b) Representative actions and DPA action

The GDPR, in Article 80, introduced the first explicit framework for collective redress for data protection breaches, as certain not-for-profit bodies may bring representative complaints to DPAs or pursue judicial remedies. There was no equivalent under the Data Protection Directive and the CJEU had previously denied one attempt at collective representational action.[808]

Two different types of representational action are conceived in Article 80. Article 80(1) is framed as an individual right to mandate, exercisable by a given data subject, and is still largely framed on individualistic terms.[809] Article 80(1), on its face, seems to have in mind an aggregation of individual concerns rather than a common pursuit of mutually affected individuals. It certainly does not seem to acknowledge circumstances when the affected data subjects might have conflicting interests or opinions on the treatment of their personal data. Article 80(2), by contrast, does not require an individual mandate, but rather allows independent complaints to data protection authorities by not-for-profits who are of the opinion that a data subject's rights have been infringed. Again, we see that the harm or illegality is still framed in terms of an individual interest,[810] and it might therefore seem that the collective envisaged by Article 80 is an aggregation of homogenous interests who are commensurably served by a representational action. Therefore, we might say that Article 80 seems best placed to respond to illegalities of processing which affect data subjects in a similar way, but may not be as well placed to respond to illegal processing of plural personal data in cases where there is differential impact or, particularly, difference of opinion on the appropriate treatment of the plural personal data. Assessment of harm associated with processing by reference to a single representative data subject might not take into account diversity of affected data subjects in plural personal datasets, though responsible representative not-for-profit may find their cases more compellingly brought if armed with evidence from a range of affected parties.

---

[808] Maximilian Schrems was denied the ability to rely on his own consumer status for choice of jurisdiction purposes in a representative class action by the CJEU, as the ability to take an action in Mr Schrems' home jurisdiction under Regulation 44/2001 was not sufficient to also bring claims assigned to him by other complainants. C-498/16 *Schrems v Facebook Ireland Ltd* (ECLI:EU:C:2018:37).

[809] In full, Article 80(1) provides: *The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.*

[810] Article 80(2) provides: *Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.* (My emphasis)

At this time, an active collective litigation environment on the basis of Article 80 has not yet materialised, and thus its potential difficult to assess. As Janciute has written, its real promise is contingent on supporting measures in other areas, at both national and EU level.[811] The new collective consumer redress package will include data protection actions, which may contribute.[812] The EU does not have a tradition of conceiving interests collectively,[813] and because Article 80 relies on Member State implementation to provide for representative actions (with national flexibility as to the scope of such actions),[814] such collective actions are still at a nascent stage, and may yet offer a valuable means to respond to some of the challenges of the individualised aspects of the GDPR. However, the collective approaches seem to be founded on an aggregative understanding of the collectives of data subjects, and therefore once again highlight that challenges may arise where data subjects' interests or preferences do not align.

5. Conclusion

This chapter has introduced the concept of plural personal data to describe datasets, either inherently plural or developed, which contain data relating to multiple persons. There has been some recognition of plural personal data by the CJEU and the ECtHR, and there is fragmentary recognition of it in the GDPR.

Plural personal data poses a number of challenges for the operation of EU data protection law, and in this chapter I have sought to highlight some of these challenges, in particular in light of certain aspects of the law which tend towards individualism. In evaluating three elements of the legal framework which have particular individual orientation; the threshold for application, the assessment of the legality of processing, and the granting of individually exercisable rights may be said to highlight some challenges with the application of the law to plural personal data. Questions arose on the reach of the GDPR, and whether its focus on individual protection and the requirement for identifiability of underlying data subjects hampers its ability to constrain abuses in the digital environment. Within the operation of the framework, I have highlighted two particular concerns. First, when the assessment of legality is framed in individually oriented terms, or a legal action is taken by an individual claimant, there is a risk that the claimant data subject or a notional archetypal data subject for the purposes of assessment may not be representative of all affected parties, and this runs the risk of legitimising processing which might be harmful to disadvantaged or minority data subjects. Second, when it comes to the reconciliation of varying interests and rights of mutually affected data subjects, there is no coherent regard for how such interests might be weighed. While part of the intent of the GDPR is to enhance individual control over one's personal data,[815] it does not seem to consider how such control might come into conflict where differences arise over the desirability of processing of plural personal data. This potential conflict highlights the manner in which data protection law envisages the individual data subject: largely separated from their fellow data subjects, self-contained and homogenous. I suggest that the challenges of the application of EU data protection law to plural personal data highlight this particular individuated conception of the data subject, often

---

[811] Laima Janciute, 'Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities' (2019) 9 International Data Privacy Law 13.
[812] DIRECTIVE (EU) 2020/1828 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409/1, 4/12/2029, p 1–27).
[813] Catherine Warin, 'Individual Rights and Collective Interests in EU Law: Three Approaches to a Still Volatile Relationship' (2019) 56 Common Market Law Review 463.
[814] Article 80, GDPR and Recital 142, GDPR.
[815] Recital 68, Recital 75, Recital 85, GDPR. See also, Chapter 2, sections 2 and 3.5; and Chapter 6.

ignoring their relationships with others which contribute to interdependent and interconnected data processing.

CHAPTER 5: THE EMPOWERED INDIVIDUAL AND DATA PROTECTION PATERNALISM

1. Introduction

The idea of individual control, or individual agency over their data is connected to the normative underpinnings of EU data protection law,[816] the role of the individual as an enforcer of EU data protection law,[817] and the challenges individual control over plural personal data can create.[818] However, it would be incorrect to classify the EU data protection regime as one of pure informational self-determination. Rather, the law combines individual empowerment and individual protection. This chapter looks to this balance between the empowerment and protection of the individual, as in doing so, seeks to incorporate questions of the conception of that individual, and the link to this balance of approaches. This chapter considers the extent to which the regime considers the individual data subject or rights-holder as an empowered person, capable of their own self-defence, versus those circumstances in which the individual is deemed in need of protection.

Empowerment is often conceived of in data protection law as a matter of consent to data processing, but this contribution offers a framework for considering the totality and extent of empowerment in EU data protection law, but using the concept of paternalism as a counterpoint. Empowering and paternalistic strategies can be identified at substantive, procedural and structural levels. In contrasting these approaches, the conception of the empowered individual which emerges is a marketized subject, and despite a prevalence of paternalistic strategies, there is no cohesive conception of the protected subject, or a paternalistic approach to data protection.

2. Empowerment and paternalism: two perspectives on data protection

2.1. Empowerment versus paternalism

In this chapter, when I refer to individual empowerment, I mean the safeguarding of an individual's autonomy through the law; i.e. an individual's capacity to self-govern.[819] As I will explain, this can occur at different levels, but I am concerned with the ways in which the legal system supports or protects an individual's autonomy. This is intentionally broader than an understanding of informational self-determination, which calls for an individual's choices over data to be secured or respected.

Paternalism, on the other hand, I use to signify the inverse to individual empowerment. I use the term paternalism to refer to the legal interference with an individual's autonomy,

---

[816] See Chapter 2, section 2; Chapter 5, section 2.2.
[817] See Chapter 2, section 3.5.
[818] Chapter 4.
[819] This chapter does not attempt to delve into the philosophical debate on the meaning of autonomy, this is beyond the scope of my thesis. As Catriona Mackenzie has written, conceptions of autonomy are contested and premised upon different assumptions about personhood. Catriona Mackenzie, 'Relational Autonomy' in Kim Q Hall and Ásta (eds), Catriona Mackenzie, *The Oxford Handbook of Feminist Philosophy* (Oxford University Press 2021). The understanding of autonomy as the capacity to govern oneself derives from the literal meaning of the Greek roots of the word 'autonomy', and at a highly general level can be said to be shared across a variety of philosophical conceptions of autonomy. See John Christman, 'Autonomy' in Roger Crisp (ed), *The Oxford Handbook of the History of Ethics* (Oxford University Press 2013) 691.

instances where data protection law interferes with an individual's self-governance. Paternalism arises in both a protective and restrictive manner under EU data protection law, protective paternalism arising when the law imposes conditions on the individual which constrain their autonomy in the name of the protection of that same individual. In other words, the law constrains individual choice "for their own good". On the other hand, paternalism can also operate in a restrictive sense, when the law imposes conditions on the individual which restrict their autonomy in the furtherance of some other objective or interest. I do not seek to ascribe a normative value to these terms, but rather adopt these labels as a means to explore the relationship between EU data protection law and individual autonomy. Finally, I note that there is a degree of artificiality in making a clean distinction between empowerment and paternalism, as some legal provisions and decisions will incorporate elements of each. There is a degree of abstraction in this line of analysis, which nevertheless can offer us a useful way to tease out the balancing between different legal strategies and priorities in the manner in which EU data protection law seeks to meet its goal of individual protection.

Questions of individual autonomy and data protection are often framed in terms of the issue of individual *control* over their personal data. As Lynskey notes, there is no unitary principle or cohesive concept of "control of data" in data protection law or scholarship.[820] Lazaro and Le Métayer observe that while this "notion of control dominates the contemporary conceptual and normative landscape of data protection and privacy" its meaning and normative implications are vague and under-studied."[821] Kaminski suggests that "control" of data is used as "a shorthand for autonomy",[822] but without agreement as to its meaning, the opacity of the concept of control can serve to obscure the nature of what individuals are obtaining under the law, and undermine our ability to meaningfully critique such "control". By focusing on empowerment as the support of individual choice or self-determination, I hope to avoid fixation on control of data as an end in itself,[823] and rather connect data protection empowerment with a truer sense of individual autonomy.[824] Secondly, by re-engaging with empowerment in the broader sense of individual choice, we must necessarily engage with both the safeguarding and withdrawal of such choice, and thus the balance between empowerment and paternalism.

I am not the first to consider this balance. Both Quelle and Lindroos-Hovinheimo have observed the tension between empowerment and protection in EU data protection law.[825] Quelle observes that this tension mirrors a dichotomy of human rights theory,[826] and

---

[820] Lynskey, *The Foundations of EU Data Protection Law* (n 86) 180.
[821] Lazaro and Le Métayer (n 310) 4.
[822] Margot E Kaminski, 'The Case for Data Privacy Rights (Or 'Please, a Little Optimism')' (2022) 97 Notre Dame Law Review Reflection 385, 7.
[823] Brownsword has so warned against the fallacy of fixation upon consent. Roger Brownsword, 'The Cult of Consent: Fixation and Fallacy' (2004) 15 King's Law Journal 223.
[824] Inspired by Rouvroy and Poullet (n 310). Rouvroy and Poullet warn against an interpretation of individual preferences over data as the final value of data protection, as obscuring and undermining the capacity of data protection to foster individual autonomy more broadly.
[825] Claudia Quelle, 'Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps*, vol 498 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-55783-0_11> accessed 3 August 2021; Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78).
[826] She argues that the balance between user control and controller responsibility mirrors the debates between will and interest based theories of rights. Quelle (n 825) 159. She argues "Under a will theory of rights, user control is indispensable, despite the constraining conditions of choice, while an interest

Lindroos-Hovinheimo argues that the conception of the person within the GDPR is primarily of a person in control, but allows for some acknowledgment of individual vulnerability or passivity within the regime, who is the subject of protection.[827] Van der Sloot has observed that the increased prominence of individual control based approaches in EU data protection law is a departure from historical emphasis on principles of good governance, grounded in ideas of reasonableness and fairness.[828] Bygrave and Schartum's weighing of consent versus proportionality based data protection is also an analogous question.[829] Ausloos frames this issue as a dichotomy; between protective and empowerment measures, between a vision of an active or passive data subject.[830]

My contribution offers an examination of the manner in which EU data protection law empowers the individual (in the sense of supporting individual autonomy) and the inverse, the manner in which the law supplants individual autonomy, in the name of individual protection or other interests, and offers a framework for articulating and assessing these aspects of the regime. This framework identifies empowerment and paternalism in the substantive, procedural and structural senses. By connecting empowerment to autonomy, the narrowness of data protection empowerment emerges. At the same time, despite the prevalence of paternalistic strategies, there is an absence of any cohesive conceptualisation of what data protection might entail in the alternative to individual self-determination. In making this assessment, the conception of the empowered individual emerges as a marketized subject, as the law borrows from marketplace conceptualisations and strategies in its approach.

2.2. The vision of EU data protection law: protection through control and paternalism

The question of the balance between empowerment and paternalism is not expressly recognised in the GDPR, but intrinsically connected to the underlying vision of the regime,[831] and how the protective aims of the GDPR and Article 8 of the Charter are translated into a regulatory framework.

The very term of "data protection" is a shorthand for "the protection of natural persons with regard to the processing of personal data".[832] In the GDPR, the idea of protection has become intertwined with the idea of control, which mirrors the central role of control over data and autonomy approaches to data protection and information privacy theory.[833] But the GDPR is much more than a "notice and choice" regime, and in many circumstances legitimisation of data processing is not a matter of individual control or choice, but grounded in other regulatory approaches. Thus, the law's notion of protection marries a safeguarding of individual choice with what we might call a more paternalistic form of protection. Moreover, as other objectives and interests also come to be balanced against the individual's interests, both in the legislative framework, and in the weighing of competing fundamental rights and freedoms, the individual's autonomy may also be restricted in order to prioritise or further other objectives.

---

theory of rights supports a large role for controller responsibility, despite the paternalism of this tenet." ibid 152.

[827] Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78) 172.

[828] van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60).

[829] Bygrave and Schartum (n 85).

[830] Ausloos (n 84) 87.

[831] See also Chapter 2, section 2.

[832] Per the title of the GDPR, in the Data Protection Directive, "the protection of individuals with regard to the processing of personal data", in the Charter "protection of personal data concerning him or her."

[833] See Chapter 2, sections 2 and 5.1, and Chapter 3, section 3.2.

The goal of individual empowerment with respect to the processing of their data receives express attention in the legislative framework, and is translated into specific legal safeguards over consent, contractual choice and individual rights of self-defence and remedies. Because of these express provisions and the historically significant role of theories of control over data,[834] we may have a clearer sense that data protection is about the protection of individual autonomy through the protection of choice.

Paternalistic approaches to data protection do not have the same cohesive narrative, and rather are a collection of approaches applicable in different contexts. Perhaps as a result, individual empowerment receives more attention while aspects of paternalistic protection are siloed into different areas of discussion (e.g. controller obligations, data protection by design, processing by public authorities etc.). Van der Sloot and Bieker are notable in pointing to these paternalistic approaches, sometimes called structural approaches, or bureaucratic approaches to data protection as an alternative to individualistic approaches.[835] I suggest that it can be fruitful and indeed necessary to examine the paternalistic elements of the law. The manner in which EU data protection law supplants choice and imposes alternative protective approaches both helps us to understand how the law positions the individual as an agent versus protected subject and also understand more deeply the balance between empowerment and paternalism within the existing framework, and the philosophical goals these strategies represent.

These questions of empowerment and paternalism within the law are connected to the individual within EU data protection law. After all, it is the empowerment or protection of the individual in question. Thus, as we shall see even from the outset, this regulatory balance reveals different understandings of the individual, based on important pre-suppositions which ground the law.

3. Empowering the individual: substantively, procedurally and structurally

The question of the empowerment of the individual within EU data protection has been subject to frequent attention, often through the lens of empowerment as the control of data. In this section, I first consider how empowerment of the individual serves as a normative ideal underpinning the GDPR. I then go on to examine how such a normative ideal is translated into the legislative scheme, and offer a new framework to understand how the legal regime purports to empower the individual; in terms of the substantive basis for data processing, procedurally and structurally.

3.1. Empowerment as a normative ideal: the individual as normative foundation and agent revisited

Empowerment is not explicitly acknowledged in the GDPR, but in the context of the GDPR's aim to protect the individual, the ideal of individual control over data does receive some attention. The stated need for "a strong and more coherent data protection framework" leads to the statement that "Natural persons should have control of their own personal data."[836] The loss of a data subject's ability to exercise control over their data is considered a risk to the rights and freedoms of natural persons which inform the obligations upon data

[834] See Chapter 3.
[835] van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60); Bieker (n 70).
[836] Recital 7, GDPR.

controllers.[837] As will be considered in the following section 3.2, the legal regime safeguards individual choices over data in a variety of fashions, through the legitimation of data processing linked to individual choice, through the grant of procedural safeguards and through structural supports to individual choice. Notably, the ECtHR have held that Article 8 of the ECHR "provides for the right to a form of informational self-determination."[838] This raises interesting questions as to whether Articles 7 or 8 of the Charter must also be interpreted as encompassing such rights, as it depends on whether "informational self-determination" offers more or less extensive protection than the protection secured by Articles 7 or 8 of the Charter.[839]

Individual control over data has been continually put forth (or indeed criticised) by academics as the normative core of data protection as a regime. This vision of individual empowerment, associated with theories of informational self-determination which first became associated with information privacy in the 1960s,[840] has become the dominant academic theory of the underlying purpose of data protection.

Bygrave's text on data protection was influential, and he articulates this vision of individual empowerment as follows: "A core principle of data protection is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations."[841] This nuanced picture of individual *participation* as opposed to *control* is notable. Later works tend to focus on control. Thus we see this in Lynskey's work, where she identifies control as the starting point, as the normative anchor of EU data protection law, but one to be reconciled with other interests and objectives, and she goes on to identify limitations associated with control based approaches.[842] Ausloos argues that control over one's personal data is "the essence" of the right to data protection,[843] with a vision of control incorporating a structural dimension. He argues that "[t]he right to data protection simply implies an environment that fosters and safeguards the ability of individuals to maintain some level of control—positive or negative—over their personal data throughout its lifecycle."[844]

The notion of individual control over data is also the starting point for a number of prominent critiques of EU data protection law. Bygrave and Schartum offer a summary of the key criticisms, taking as their starting point consent as an individualised mechanism of data

---

[837] Recital 75, 85, GDPR. Opinion of Advocate General Campos Sánchez-Bordona has interpreted these statements such that strengthening control as "one of the recognized aims of the modernization of the rules on the protection of personal data, albeit not an independent or isolated aim." C-300/21 *Österreichische Post AG* Opinion of Advocate General Campos Sánchez-Bordona 6 October 2022 (ECLI:EU:C:2022:756).

[838] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR, 27 June 2017), para 137. The ECtHR have also identified rights of an individual to control the use of their image as an essential component of personal development, in the context of photographs. *Reklos and Davourlis v Greece* App no 1234/05 (ECtHR, 15 January 2009), para 40; *Von Hannover v Germany (No. 2)* Apps nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), para 96.

[839] In accordance with the position in Article 52(3) of the Charter which provides that "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection." See also Chapter 2, section 2.2(a). This question is reserved for future work.

[840] See Chapter 3, including the influence of Alan Westin's theory of informational privacy as control over data.

[841] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 18) 87.

[842] Lynskey, *The Foundations of EU Data Protection Law* (n 86) 254–257.

[843] Ausloos (n 84) 61.

[844] ibid 62.

protection.[845] These limitations include: legal difficulties with interpreting consent, extra-legal factors which undermine privacy interests (e.g. monopoly operators), information imbalances, and "problems of consensual exhaustion, laxity and apathy".[846] At the same time, they are not fatalistic as to control mechanisms, which can have "bite",[847] and balance this against structural/proportionality based approaches which can vary in their effectiveness according to context.[848] Others go further, and dismiss entirely control based approaches. Lazaro and Le Métayer have criticised control as self-determination approaches.[849] Bietti has also argued for such a re-orientation away from control, consent and choice.[850] Lindroos-Hovinheimo associates control with an ideology of possessive individualism and argues for a reinterpretation of privacy away from such ideas.[851]

Considering this normative ideal of individual control over data so often seen in the academic literature and as well as in public discourse, this might give the lay person the idea that data protection law's primary function was to secure such control. Indeed, an individual's choices over data processing are subject to direct legislative attention and protection. In this section, I examine how the law safeguards individual choices over data processing, the limits of such safeguarding, and all the while remembering that this legal empowerment is only part of a larger regime.

3.2. Legal empowerment of the individual

An individual's choices are safeguarded under EU data protection law in three senses.[852] First, an individual's choices over the substantive basis for data processing are safeguarded through the legitimation of consent and contract-based processing. Second, the individual is armed with a series of rights which they may exercise to defend their data protection interests, which may be considered a type of procedural empowerment of individuals. Third, an individual may be indirectly empowered, as data controllers are bound to consider individual loss of control over data when performing their obligations, and thus the law might be said to contribute to a structural empowerment of individuals.

(a) Substantive empowerment

EU data protection law may be said to empower individuals in the sense of protecting their choices over the substantive basis for data processing. This empowerment, in terms of respecting an individual's choice over the purpose of data processing is contained in Article 6 of the GDPR, which provides six exhaustive bases for data processing. Two of these

---

[845] Bygrave and Schartum (n 85).
[846] ibid 160–161.
[847] ibid 166.
[848] ibid.
[849] Lazaro and Le Métayer (n 310).
[850] Bietti's focus is on discourses of consent and control, and thus as she recognises the emphasis on consent and control may be temporary. Her thesis that data protection enforcers focus overly on consent and control is limited due to limited transparency / empirical data on enforcement activities, nor indeed upon the organisational compliance practices of data protection. Bietti (n 86).
[851] Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (n 78).
[852] Lynskey grounds her finding of individual control in the data subject rights (which I characterise as procedural empowerment). Lynskey, *The Foundations of EU Data Protection Law* (n 86) 180 et seq. Ausloos equates empowerment with control over data and primarily focuses upon the data subject rights. Ausloos (n 84) 88. My conception of individual empowerment extends beyond arming data subjects with new rights, encompassing also safeguarding/legitimising individual choices over data, as well as the environment of data processing created by the GDPR, and thus also consider what I call 'substantive' and 'structural' empowerment below.

mechanisms are grounded in legal recognition of an individual's choice: consent to data processing and the legitimisation of processing on the basis of contractual necessity.

Consent is often put forward as central to data protection. Usually, the significance is linked to ideas of control over data and the purpose of data protection.[853] A characteristic example of such an argument is seen in Bygrave and Tosoni's position that "[c]onsent by persons to the processing of data relating to them lies at the heart of the ideals of personal autonomy and privacy, particularly when these are conceived in terms of 'informational self-determination."[854] In such a characterisation, consent is central to EU data protection law because it is the legislative implementation of individual empowerment over their data. We see such a characterisation explicitly endorsed by Advocate General Spunzar in *Orange Romania,* wherein he writes that:

> "[t]he guiding principle at the basis of EU data protection law is that of a self-determined decision of an individual who is capable of making choices about the use and processing of his or her data. It is the requirement of consent which enables him or her to make this choice and which at the same time protects him in situations which are by their very nature asymmetrical."[855]

Consent also seems to takes prominence in public discourse on data protection. While I do not purport to precisely diagnose why consent uniquely attracts such attention amongst the six legal bases for data processing, perhaps it may connected to the familiarity and accessibility of the concept, in an otherwise complex and opaque legislative scheme. Consent is a familiar concept within many legal systems. As Kosta writes, "[c]onsent is a notion engrained in the very fabric of civil law."[856] Brownsword has also observed that a notional commitment to consent is reflected in much of English law.[857] Consent is familiar to us through practices and laws of medical consent,[858] laws and norms relating to consent to sexual conduct and as a market concept, supporting the conclusion of contracts. At a deeper level, consent has been connected "to the basis of legal authority and perhaps to the essence of legal order itself" according to liberal theorists, as Beyleveld and Brownsword

---

[853] For example: Curren and Kaye write "an individual's consent to use their personal information is the primary means for individuals to exercise their autonomy and to protect their privacy." Liam Curren and Jane Kaye, 'Revoking Consent: A "Blind Spot" in Data Protection Law?' (2010) 26 Computer Law & Security Review 273, 274. Kosta writes that consent was introduced into data protection law "in order to enhance the role of the data subject in the data protection arena and to strengthen his control over the collection and processing of his personal information." Kosta, *Consent in European Data Protection Law* (n 229) 397.

[854] Lee A Bygrave and Lee Tosoni, 'Article 4(11). Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 176.

[855] Case C-673/17 *Planet49* Opinion of Advocate General Szpunar 21 March 2019 (ECLI:EU:C:2019:246), par 37. However, the CJEU does not adopt this language, even where it follows the Advocate General's approach to consent. C-673/17 *Planet49* (ECLI:EU:C:2019:801).

By contrast, Advocate General Campos Sánchez-Bordona rejects such an approach, rather advising that "the GDPR does not seek to increase the control of individuals over information concerning them, by merely giving way to their preferences, but rather to reconcile each person's right to protection of personal data with the interests of third parties and society. The aim of the GDPR is not, I stress, to limit systematically the processing of personal data but rather to legitimise it under strict conditions." C-300/21 *Österreichische Post AG* Opinion of Advocate General Campos Sánchez-Bordona 6 October 2022 (ECLI:EU:C:2022:756), paras 81-82.

[856] Kosta, *Consent in European Data Protection Law* (n 229) 382.

[857] Brownsword (n 823).

[858] Indeed, Kosta argues that consent as formulated in the Data Protection Directive was closely linked to the rights-based approach to consent in bioethics based on informed consent to clinical trials Kosta, *Consent in European Data Protection Law* (n 229) 385.

have written.[859] In the fundamental rights sphere, consent does much work, both functionally and normatively. Consent can offer a legal basis for the interference with fundamental rights[860] and consent is central to the conceptualisation and justification of a number of fundamental rights, particularly those concerned with autonomy.[861] Fundamental rights are central to the EU's data protection regime, and this rights-driven approach to EU data protection law grounded Brownsword's defence of a necessary continuing role for individual consent within data protection law.[862]

Certainly, consent has important significance within the regime. Consent is the only legal basis for processing named in Article 8 of the Charter,[863] and might even seem to be the default legal basis under the Charter. Nevertheless, as consent's only direct legal significance is as a legal basis for processing,[864] its position in academic scholarship and public discourse seems somewhat outsized.[865] As Gil Gonzalez and de Hert have observed, within the GDPR itself "[n]o single basis is better than others, and there is no hierarchy among the six grounds."[866] At the same time, in areas of perceived heightened risk, where the GDPR implements additional special rules, consent also has a role in legitimating such exceptional forms of data processing. Consent is also a ground to legitimise processing of special categories of data,[867] automated decision making[868] and transfers of data outside the European Economic Area,[869] in each case requiring the higher threshold of *explicit* consent.

Legally, consent is narrow and exacting; with high standards applied to the required criteria of "freely-given", "specific", "informed" and "unambiguous indication", and recent emphasis on the need for "active" consent by the CJEU.[870] Clarifications inserted by the GDPR only

---

[859] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 3.
[860] According with a will/choice theory of rights, as Brownsword and Quelle have observed. Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009); Quelle (n 825).
[861] Particularly the right to marriage (Article 16, United Nations Declaration on Human Rights), the right to dignity in healthcare (Article 6, Universal Declaration on Bioethics and Human Rights), the right to integrity of the person (Article 3, Charter) and of course, the right to privacy.
[862] Brownsword (n 860).
[863] Article 8(2) provides: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
[864] Article 6(1)(a), GDPR.
[865] Bietti has argued that regulators in particular have paid "disproportionate" attention to the concept. Bietti (n 86) 3. Arguably, this may have reflected data controller's disproportionate reliance on consent as a legal basis for processing.
[866] Elena Gil González and Paul de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (2019) 19 ERA Forum 597, 599.
[867] Article 9, GDPR. Of additional interest is the provision that renders processing special categories of personal data lawful where the data has already been "manifestly made public by the data subject", which suggests a similar idea of the data subject choosing to put such information into the public sphere and thereby losing the additional protection of Article 9.
[868] Article 22, GDPR.
[869] Article 49(1)(a), GDPR.
[870] See Case C-673/17 *Planet49* Opinion of Advocate General Szpunar 21 March 2019 (ECLI:EU:C:2019:246), paras 61-62, 72-73; and Case C-673/17 *Planet49,* the CJEU stating that "Only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement." C-673/17 *Planet49* (ECLI:EU:C:2019:801), par 54. See also C-61/19 *Orange Romania* (ECLI:EU:C:2020:901), para 35.

confirm such a strict approach.[871] Bygrave has defended this strict approach, on the basis that it "serves to ensure that […] autonomy is not undermined by contractual or quasi-contractual mechanisms that reflect significant imbalances of market power between service providers and their customers."[872]

Consent may thus be said to empower an individual in the sense of securing their choices over data. This empowerment, however, in the words of Bygrave and Schartum is "substantially diminished by the fact that consent tends to just be one of several alternative preconditions for data processing."[873] Thus, while the legal recognition of consent as a basis for data processing may legally recognise a decision of a data subject, the absence of such a consent is not necessarily fatal to the data processing, as the controller may have recourse to another legal basis in the alternative. Beyond this limitation, the strictness of the formulation of consent might also be characterised as protective in a paternalistic sense; as we shall consider further below, consent is deemed inappropriate in a wide set of circumstances.

Alongside consent, the legal basis of contractual necessity bears a close relation to the idea of individual choice over data processing,[874] and in this sense may be regarded as connected to the empowerment of the individual data subject. The notion that consent and contractual necessity are connected by the idea of control over data is seen in the scope of the right to portability, that right only applying to data which was processed on the basis of consent or contractual necessity.[875] This is reinforced by Recital 68 which locates the data subject's right to portability in the need "[t]o further strengthen the control over his or her data".

Contractual necessity bears the same idea of respecting an individual's choice as consent; in this case, a choice to form a contract. Beyleveld and Brownsword connect the law of contract to the notion of consent through the understanding of contract "as a consensual transaction", based on a choice of two or more parties to enter into a binding relationship with one another.[876] This understanding of contracting as a free exercise of individual choice can be said to relate to a notion of individual empowerment which underlies control based processing, and subject to many of the same critiques.

---

[871] Article 7, GDPR, and special rules regarding certain children's consent in Article 8, GDPR. Legislators were aware of concerns relating to consent under the Data Protection Directives, leading to the addition of Article 7 of the GDPR. Bygrave and Tosoni (n 854) 177. These legislative additions have been stated to be clarifications rather than additions by Bygrave and Tosoni, ibid 181. Indeed Advocate General Szpunar in *Planet49* stated that the requirements for giving consent under the GDPR are the same as the Data Protection Directive, though the CJEU in the same case observe the formulation in the GDPR "appears even more stringent.". Case C-673/17 *Planet49* Opinion of Advocate General Szpunar 21 March 2019 (ECLI:EU:C:2019:246), par 3; C-673/17 *Planet49* (ECLI:EU:C:2019:801), para 61. Moreover, divergent regulatory practices and conceptions of consent in different Member States under the Data Protection Directive have been identified by Kosta (Kosta, *Consent in European Data Protection Law* (n 229) 386.) As such, the GDPR amendments may represent some degree of change, through greater harmonisation of the standard of consent and through clarification of the requirement of active consent.

[872] Lee A Bygrave, 'Article 4(11). Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles* (Oxford University Press 2021) 47 <https://www.ssrn.com/abstract=3839645> accessed 16 November 2021.

[873] Bygrave and Schartum (n 85) 161.

[874] Article 6(1)(b) of the GDPR provides that processing may lawful if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

[875] Article 20, GDPR.

[876] Beyleveld and Brownsword (n 859) 3.

In these ways, consent and contractual necessity both operate to grant legal status to an individual's choice, and in this way can be said to be a legal empowerment of individuals. Once in place as the relevant legal basis for processing, the individual's choice is further safeguarded through the principle of purpose limitation.[877] Consent and contractual necessity as a basis for processing are probably the closest the GDPR comes to implementing informational self-determination, in the sense that the individual is the one who determines the use of their data. Whether this is truly an empowerment of the individual in the sense of safeguarding their autonomy is a matter for further consideration in section 5 below.

(b) Procedural empowerment

Data protection law grants individuals a series of rights, some exercisable against data controllers and some enforcement rights to be pursued before a DPA or judicial authority. These rights vary in nature, and will be reintroduced in brief below. I suggest that the extent to which these rights empower individuals in the sense of safeguarding an individuals' choices similarly varies, and we can see a spectrum from important measures of individual choice (at least formally), to other rights which are rather narrower in terms of possibility. The rights to access and portability are important tools to allow individuals to oversee the treatment of their data and exercise choice. The right to objection offers an important means for the data subject to inject their views into ongoing processing scenarios. However, I argue that some of the data subject rights are more properly seen as a procedural defence against law-breaking, and at best reinforce prior individual choices.

An individual data subject is granted a series of rights which may be exercised against a data controller; the rights of access, rectification, erasure, restriction, data portability, objection, and not to be subject to automated decision making.[878] Often these rights are classed as safeguarding individual control over data.[879] However, when we reflect upon empowerment in the sense of individual choice (and perhaps even the narrower sense of choice over data), I suggest that the empowering potential of many of the data subject rights is more limited.

The right of access to one's data from a controller,[880] attracts particular attention as a foundational or core right.[881] This right is certainly connected to individual choice, and we might think of it as facilitative of such choice. Alongside data controller transparency notices,

---

[877] As stated in *Digi* in assessing purpose limitation there must be "a specific, logical and sufficiently close link between the purposes for which the personal data were initially collected and the further processing of those data, and ensure that such further processing does not deviate from the legitimate expectations of the subscribers as to the subsequent use of their data." C-77/21 *Digi* (ECLI:EU:C:2022:805), para 36. See also Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86) 14.

[878] The right not to be subject to automated decision making, while a right in name, has been largely interpreted as a prohibition, which does not require the individual data subject to claim it, before it comes into effect. 'Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679' (Article 29 Working Party 2017) WP251. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision making-and-profiling_en, p 19.

For this reason, I exclude it from the data rights in discussion here, the remainder of which require individual action, and thus may be classified according to a spectrum of empowerment.

[879] See for example Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation' (n 86); Lynskey, *The Foundations of EU Data Protection Law* (n 86); Ausloos (n 84).

[880] Article 15, GDPR.

[881] E.g. Lynskey, *The Foundations of EU Data Protection Law* (n 86) 181–185; Mahieu (n 84).

the right of access provides individuals with the information to inform individual choice, and to detect illegality in order to allow individuals to defend their interests.[882]

The right to portability might also be said to be connected to individual choice, and the provision of a new entitlement to protect such choice. The right to portability protects an individual's right to transmit their personal data from one controller to another.[883] This might be seen to connect with an individual's consumer choices,[884] to move from service provider to another and have their data transmitted to support such a choice.

The right to objection allows for an individual to assert their interests in a less substantive way, as they are not exercising a proactive choice about their data, and yet may be an important means of participating in the decision making process by asserting their particular circumstances and interests. The right arises where the data subject's interest was to be weighed in the original assessment of legality (on the basis of public interest necessity or the data controller's legitimate interests).[885] The objection is to be successful unless the data controller demonstrates their overriding grounds to continue data processing (which a data controller was already bound to do before they commenced processing, by virtue of their accountability burden and the terms of the public interest and legitimate interest processing bases). In this sense, the individual's exercise of the right to objection may force the controller to consider that individual's particular case; their circumstances, rights and views, a more meaningful participation than might otherwise have occurred when the balancing exercise conducted is in the hands of the controller.

The rights to rectification, erasure, and restriction, on the other hand, have less to do with safeguarding an individual's choices than arming the individual with a basis to defend their interests when unlawful processing occurs. Ausloos characterises these rights as *ex post* empowerment,[886] and in particular argues that the data subject rights (particularly objection, erasure and rectification) are the main way in which the data subject is empowered under the GDPR (which he categorises as data subject control over data). However, when we consider individual empowerment in the sense of safeguarding an individual's choices or self-determination, these rights cannot be characterising as empowering an individual beyond defending themselves against illegality.

Once we consider the scope of the rights to rectification, erasure, and restriction, it becomes clear that they are exercisable in circumstances where the processing of the data in question by the data controller is already contrary to the GDPR. The right to rectification grants an individual the right to obtain the rectification of inaccurate personal data.[887] Data accuracy is already a data protection principle which the data controller is required to comply with.[888] The

---

[882] Confirmed by the CJEU in *RW v Österreichische Post AG,* wherein the Court stated that the "right of access must enable to data subject to verify not only that the data concerning him or her are correct, but also that they are processed in a lawful manner… and in particular that they have been disclosed to authorised recipients." C-154.21 *RW v Österreichische Post AG* (ECLI:EU:C:2023:3) para 37.

[883] Within the terms of Article 20, GDPR.

[884] The right is only available where the data processing is justified on the basis of consent or contractual necessity. See Article 20(1)(a), GDPR.

[885] Article 21(1), GDPR.

[886] Ausloos (n 84) 72.

[887] Article 16, GDPR.

[888] Article 5(1)(d) GDPR requires that personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')".

right to erasure is exercisable where personal data is no longer necessary for its original purpose, consent has been withdrawn, a successful data subject objection has been made, data has been unlawfully processed, data must be erased to comply with a legal obligation or where a child's data was processed in relation to an offer of information society services.[889] Each of these bases accords with a form of illegal data processing. If the data is no longer necessary for the original purpose, under the principle of storage limitation the controller should be erasing or anonymising such data in any case.[890] If consent has been withdrawn, the controller has been deprived of the legal basis for the processing of such data. If the data subject's objection has been successful, then the data controller's reliance on the legitimate interest or public interest ground to justify data processing was improper—the controller's interest did not override the interests of the data subject.[891] This is at its most clear when you consider the right to erasure is available when personal data is unlawfully processed or the data must be erased for compliance with a legal obligation, and thus clearly in both these cases, the data controller is continuing to process this data illegally. The right to erasure is also available in relation to information society services where consent was obtained from a child or their parent/guardian, and thus could be regarded as available where the original legal basis for processing is no longer appropriate. The same analysis is true of the right to restriction, which grants an individual a right to obtain restriction of processing where the lawfulness of the data processing is under contestation; because data accuracy is challenged or an objection has been made,[892] or where the data processing is unlawful but the data subject wishes the data to be preserved.[893]

Thus I suggest the rights to rectification, erasure, restriction and objection have more in common with an individual's procedural rights to complain to a DPA, or to pursue a judicial remedy. Certainly, potentially valuable as part of the wider enforcement tool-box,[894] and we might say a narrow legal empowerment in the sense of the creation of individual mechanisms for redress,[895] but nevertheless appears narrower in the sense of a true empowerment of individual autonomy, as is considered further in section 5 below.

(c) Structural empowerment

The final way in which EU data protection law might be said to empower individuals is indirectly, by placing responsibility upon data controllers (and sometimes national legislators) to be transparent in their practices and to safeguard against individuals' loss of control over data. This indirect empowerment might be thought of as a type of structural empowerment, as controllers and legislators are bound to contribute to an environment within which individual choice is facilitated and respected.

---

[889] Article 17(1), GDPR. There are overriding exceptions in Article 17(3) which allow the controller to deny the erasure request.
[890] Article 5(1)(e), GDPR.
[891] Per Article 21, GDPR: "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."
[892] Articles 18(1)(a) and (d), GDPR.
[893] Articles 181)(b) and (c), GDPR.
[894] See Lauren Henry Scholz, 'Private Rights of Action in Privacy Law' (2022) 63 William and Mary Law Review 58. Kaminski's defence of individual privacy rights is also at its most credible in relation to this enforcement/governance role for individual rights. Kaminski (n 822).
[895] See Chapter 2, section 4.2.

An individual may only make decisions about the processing of their data if they are armed with the information to do so. The transparency obligations with which data controllers must comply thus play a role in supporting individual decision making.[896] Notionally, individuals can review a wide array of information about how controllers propose to deal with data before the individual chooses to engage with that controller, or to assert their interests in the case of illegal data processing. In this way, the transparency obligations within the GDPR serve as an indirect empowerment to individuals, by ensuring data subjects are aware of, or may choose to become aware of, the practices of data controllers.

Further, by mandating that a controller must have regard to loss of control by individuals, we see further indirect empowerment of individuals. A controller's obligations must be exercised with reference to the "risk to the rights and freedoms of natural persons,"[897] which has led to Gellert's work on the possibilities of risk-based approaches to data protection.[898] One of the risks expressly named in the Recitals which controllers are bound to consider is the risk that data subjects might be "prevented from exercising control over their personal data."[899] Controllers are further obliged to consider this risk (amongst others) in performing data protection by design,[900] and conducting data protection impact assessments.[901] In addition, where national legislatures are restricting the operation of the GDPR's obligations as permitted by way of national legislative derogation in certain cases, they too must have regard to and specifically legislate for this risk of loss of control.[902]

In this way, at least formally the law might be said to contributing indirectly to individual empowerment by requiring controllers to be transparent in their practices, and mandating that legislatures and controllers must avoid curtailing individual control over data. This may be the type of protection Ausloos has in mind when he advocates for an understanding of control inherent to the right to data protection which goes beyond individual responsibility and which "implies an environment that fosters and safeguards the ability of individuals to maintain some level of control—positive or negative—over their personal data throughout its lifecycle."[903] Similarly, when Bieker makes a normative case for a dualistic vision of the right to data protection, which incorporates both individualistic and structural components, draws on the principles of both control and fairness, amongst others, in his conception of this structural component of data protection.[904]

Thus, when we think of the ways in which the EU data protection law supports or facilitates individual empowerment, it can be helpful to differentiate the levels at which this support occurs. We can see levels of support for individual choice or participation in the processing of data, at the substantive level, when individual choices are given legal status in legitimating data processing, at the procedural level, when individuals are armed with rights to exercise against data controllers when concerned as to the use of their data, and finally at a structural

---

[896] Articles 12-14, GDPR prescribe information to be provided by data controllers, along with Article 5(1)(a), GDPR requiring data subjects to process data *inter alia* in a **transparent** manner.
[897] Article 24(1) of the GDPR provides: "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."
[898] Gellert (n 143); Gellert (n 148).
[899] Recital 75, GDPR.
[900] Article 25(1), GDPR.
[901] Article 35, GDPR.
[902] See Article 23, GDPR.
[903] Ausloos (n 84) 64.
[904] Bieker (n 70).

level, when we see obligations upon controllers which are aimed at creating a wider environment in which individual choice and control are respected. What these tiers of support for individual choice add up to, in terms of contributing to a true sense of individual empowerment will be examined in section 5 below.

4. Data protection paternalism: "protecting" the individual data subject, whether they like it or not

A discussion of legal empowerment of the individual in EU data protection law is not complete without the other side of the legal approach: those elements of the law which seek to constrain choice, usually in the name of protecting that individual, though sometimes to defer to the interests or rights of another.

As Bygrave and Schartum have observed, the individual is not the only decision-maker in the data protection regime: data protection authorities and data controllers have a role to play,[905] and to this list we might also add the judiciary and legislators at both the EU and national level. For this reason, in Chapter 2, I have characterised the individual as *an* agent of the GDPR, not *the* agent of the GDPR.

A number of scholars have engaged with this corollary to individual choice, as data protection and privacy laws have always existed in tension or balance with other rights and interests. Solove takes a negative conception of paternalism as an alternative to consent-based privacy self-management, arguing that "[p]rivacy scholars must identify a conception of consent that both protects privacy and avoids paternalism."[906] He counsels against paternalism, on two bases – first, that it represents a restriction on individual freedom and autonomy, and second, that there are social benefits to data analysis, which therefore should not be overly restricted.[907] This idea of restriction of individual freedom of choice was also criticised by Cavoukian et al, as they too argued against a paternalistic approach.[908] Allen is notable, her work *Unpopular Privacy* is explicitly based on a normative case for paternalistic approaches to privacy.[909] Yet her paternalism is relatively restrained in comparison to established approaches in Europe, her aim is merely to prevent individuals from revealing more than is unwise, as she argues that "privacy is so valuable that individuals must sometimes be guided—and if necessary and potentially effective, forced—to accept it for the good it does them or others."[910]

On the other hand, in the face of concerns about the viability of individualistic approaches (particularly individual control approaches), other scholars have reached to alternatives to individual choice based approaches. Given that the EU system has always balanced consent with other legitimating bases,[911] perhaps it is unsurprising that scholars are more ready to recommend greater emphasis on those aspects of the regime to counter-balance limitations associated with consent. Thus we see Lynskey exploring the possibility of a

---

[905] Bygrave and Schartum (n 85) 159.
[906] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 45) 1894.
[907] ibid 1896.
[908] Ann Cavoukian, Alexander Dix and Khaled El Emam, 'The Unintended Consequences of Privacy Paternalism' (Information and Privacy Commissioner, Canada 2014) 4.
[909] Anita L Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press 2011).
[910] ibid 25.
[911] See Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip E Agre and Marc Rotenberg, *Technology and privacy: the new landscape* (MIT Press 1997); Bygrave and Schartum (n 85); van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60).

greater role for the data protection principles,[912] Clifford and Ausloos recommending more emphasis on the principle of fairness,[913] or Zanfir arguing for the place of "safeguards" as an alternative to consent.[914] While these scholars do not explicitly categorise these approaches as paternalistic, they do represent a move away from individual choice.[915] Matzner et al are clearer in locating their alternative to individual choice and responsibility to state responsibility.[916]

This discussion can be advanced by teasing out the balance between those provisions of the law which are oriented towards individual choice and self-government and those which seek to supplant such choice. In this section, I examine the circumstances in which EU data protection law delegates decisions about data processing to entities other than the data subject, in what I label a paternalistic approach. Once again, we can classify this paternalism as taking three forms: substantive paternalism (where the choice as to the basis of data processing is made by someone other than the individual), procedural paternalism (where the outcome of a complaint or legal action over wrongdoing is dependent on a public decision-maker) or structural (where the law creates an environment in which individual choice is not determinative or respected).

4.1. Substantive paternalism

When it comes to the purposes of data processing, most of the legal bases under Article 6 of the GDPR for processing are to be determined either by the controller or legislator. We see this in two ways: first, because of limitations placed upon relying upon consent in many cases, and second, because of the central position of the controller or legislator in the determination of the majority of legal bases of data processing. This placing of the controller or legislator at the heart of the proactive assessment of the legality of data processing is also reflected in the data principles and controller obligations, but for the purpose of illustration, the legal bases are subject to further analysis in this section.

While the legal basis of consent has been put forward as a basis for claiming that the GDPR empowers individuals with regard to the processing of their data, I have already noted how the strictness of its interpretation limits its suitability for many circumstances. In addition to this strict interpretation, consent is further limited by legislative and regulatory guidance which indicates its limited utility in the context of certain relationships. Where there is an imbalance in the relationships between the controller and data subject, consent will usually not be regarded as freely given and therefore is invalid.[917] The GDPR specifically names this where the controller is a public authority,[918] and to this the regulatory guidance adds employer/employment relationships.[919] These limitations have the effect of largely excluding

---

[912] Lynskey, 'Delivering Data Protection' (n 249).
[913] Clifford and Ausloos (n 432).
[914] Gabriela Zanfir, 'Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014).
[915] Interestingly, Clifford and Ausloos categorise fairness as achieving a type of 'collective control', though perhaps a collective protective effect is a more accurate labelling. Clifford and Ausloos (n 432) 183.
[916] Matzner and others (n 310).
[917] Recital 43, GDPR.
[918] Recital 43, GDPR.
[919] 'Guidelines 05/2020 on Consent under Regulation 2016/679' (European Data Protection Board 2020) Version 1.1. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> , p. 9.

individual empowerment over the purposes of data processing within many arenas of every day (one's working life and engaging with essential and public services).

In such circumstances, the law largely accepts a status quo of power imbalance, and its protective impulse thereby takes a paternalistic slant. As the European Data Protection Board writes, with regard to public authorities: "in most cases … the data subject will have no realistic alternatives to accepting the processing (terms) of this controller."[920] One could imagine alternative legislative strategies which aimed at challenging the existence of power imbalances, or supporting collective bargaining strategies in such relationships,[921] but the GDPR does not seem to have such ambitions.[922] In circumstances where individuals are at a disadvantage and therefore unable to freely consent, the GDPR moves to find the justification for data processing in other provisions. As we shall see, there is an argument that those alternative justifications tend to place the controller at the centre of the legality of processing determination. Thus, the more powerful party in the relationship, who could not be trusted to administer and obtain free individual consents, is often deputised by the GDPR to assess and determine the purposes of data processing. While all data may not be legally conducted, and the Article 6 bases for legitimate data processing are not intended to provide a shopping list of justifications, we can nevertheless imagine controllers and legislators who have an incentive to gather data will shift to an available alternative, particularly when any ex post review of that basis may be some time coming. Thus, the consequence of a paternalistic protective approach–restraining reliance on choice where it might be coerced or unfair, arguably leads to another set of challenges in protection, that of relying on controllers who are incentivised to find a basis for processing to judge the appropriate basis.

Thus, in the alternative to consent or contractual necessity, the remaining legal bases for data processing are all within the purview of the legislator or data controller. When it comes to the prospective analysis of the legality of the purpose of data processing, it will be the legislator or data controller who controls the assessment.

Processing of data on the basis of legal obligation[923] or public interest[924] will generally be determined by national or EU legislator, as legal obligations which bind a controller or public tasks to be performed by public entities will ordinarily be defined in legislation.[925] These legal bases are said to be the most appropriate for public sector controllers (as consent and

---

[920] ibid.

[921] Bygrave and Schartum have explored this idea of creating collective consent mechanisms. Bygrave and Schartum (n 85). Others have imagined or simulated data commons for a similar purpose. Wong, Henderson and Ball (n 725).

[922] This is not to say the wider EU data protection project may not seek to tackle this in the future – the Proposed Data Act for example seems to be oriented towards reshaping data-driven markets. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data 2022/0047 COM(2022) 68 final (COD). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN

[923] Article 6(1)(c) provides for processing where "necessary for compliance with a legal obligation to which the controller is subject."

[924] Article 6(1)(e) provides for processing where "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

[925] While 'legal obligation' is not defined as a statutory legal obligation, as Kotschy points out, the antecedent under the Data Protection Directive was understood as deriving from a public legal provision rather than private obligation. Waltraut Kotschy, 'Article 6. Lawfulness of Processing' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 332. Moreover, contractual obligations are already captured by Article 6(1)(b). Recital 41 provides that this is not necessarily required to be parliamentary act, but at the same time Recital 45 requires that the purpose of processing should be determined in Union or Member State law.

legitimate interests are not ordinarily available to such controllers), though of course legal obligations which require the processing of data also apply much more broadly (e.g. taxation obligations, labour law obligations, record keeping obligations in healthcare, financial services, to name but a few).[926]

In the alternative, processing can be carried out where necessary to protect the vital interests of the data subject.[927] The legal basis is ordinarily thought of as applicable in narrow, emergency situations (by contrast to routine healthcare, for example). However, in the Recitals a broader use case of this ground is also mentioned in the sense of processing for humanitarian purposes (including monitoring epidemics), though in the past the Article 29 Working Party has advised that this legal basis should have a limited application and restrictive interpretation.[928] The "special problem" of the data subject in such instances is raised by Kotshcy, who points out that unlike under Article 9 which concerns special categories of personal data, "Article 6(1)(d) does not mention that the decision to process may be taken by the controller only if the data subject is incapable of consenting."[929] Kotschy suggests that consultation is appropriate under the principle of fair processing,[930] however, by contrast, the Article 29 Working Party advised that where consultation is possible, consent should be sought where practicable, and vital interests should be relied upon only in cases of immediate threat to the data subject.[931] Thus, by its very nature, the vital interests ground is appropriate in circumstances where individual self-determination is unlikely, and should also be regarded in that sense as a paternalistic legal basis for processing.

The final available legal basis for data processing, that of legitimate interests involves a weighing of the controller's legitimate interest versus the rights and freedoms of the affected data subject.[932] A variety of grounds may be considered "legitimate" interests, and the GDPR makes specific mention of fraud prevention, direct marketing, intra-group data sharing, and certain security practices),[933] and the impact upon the data subject must be weighed against such interests. Importantly, when considering this balance between empowerment and paternalism, as Kotschy points out, the principle of accountability mandates that the assessment of legitimate interests "must be done before starting any processing operation", and "in a proactive way, explore the likely protection interests of the data subjects."[934] Thus, once again, the legitimate interests ground must be considered to be paternalistic in the sense of supplanting the individual's decision making power; while the individual interest is

---

[926] This is certainly not to say individual interests are irrelevant to such determinations (as discussed in Chapter 2, section 3.2(b), such legislation may be reviewed by reference its interference with the rights to data protection or respect for private life under Articles 7 and 8 of the Charter), however, the individual does not have any legal means to proactively participate in such determinations, with the exception of broader democratic participation.

[927] Article 6(1)(d), GDPR.

[928] 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Article 29 Working Party 2014) 844/14/EN 20 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 17 March 2022.

[929] Kotschy (n 925) 334.

[930] ibid.

[931] 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 928) 20.

[932] Article 6(1)(f) allows processing where it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[933] Recitals 47-49, GDPR.

[934] Kotschy (n 925) 338.

foremost in the calculus, it is the controller which is made responsible for conducting the assessment and determining the lawfulness of the data processing. Individual protection is not for the individual to self-determine, but rather for the controller to consider and determine.

As noted at the outset of this section, the paternalism seen in the application of these legal bases for processing is also reflected in the data protection principles and data controller obligations, which are targeted at the controller to comply with and which (based on the accountability principle) it is for the data controller to assess and demonstrate compliance with in the first instance. This demonstrates an allocation of decision making roles regarding the substance of data processing within the law: aside from those aspects of individual empowerment highlighted in section 3 above, decisions as to how data processing is to be conducted are primarily the responsibility of the data controller. Within the constraints of the GDPR, it is the data controller who is to proactively assess data processing.

4.2. Procedural paternalism

When we consider the procedural and enforcement mechanisms within EU data protection law, it is unsurprising that most of these provisions may be characterised as paternalistic. Remedies and regulatory supervision are not designed to allow individuals to self-govern, but rather to offer those individuals the protection of the state (in various forms) when their rights and legally protected interests have been infringed.[935]

Thus, even where the individual is the instigator of the legal process (by making a complaint to a data protection authority,[936] or to a judicial authority,[937] or mandating a not-for-profit entity to act on their behalf[938]) they do not have any power over the outcome of that legal process, beyond the usual procedural rights to participate and make representations to the decision making authority. Rather, *ex post* enforcement actions will be determined by a public authority: either data protection authority or judicial authority.

A data protection authority, as part of its role in supervising the application of EU data protection law in its jurisdiction, has power to *inter alia* conduct investigations and handle complaints, and exercise corrective powers and impose sanctions.[939] Its legal role and power is interpreted in terms of the importance of protecting individuals,[940] but in this paternalistic sense, without acceding to their choices but adjudging according to its role and expertise. Courts may be called upon to resolve complaints brought against controllers, processors or data protection authorities.[941] Thus, to the extent that there are decisions being made about data processing (e.g. whether controllers can rely upon a consent to continue processing data,[942] or whether it is truly "necessary" to process data,[943] whether a legislative measure

---

[935] Article 8 of the Charter is notable in explicitly mandating a role for independent supervision.
[936] Article 77, GDPR.
[937] Article 78-79, GDPR.
[938] Article 80, GDPR.
[939] Article 55-58, GDPR.
[940] See in particular *Schrems I* and *Schrems II.* In these cases we see the CJEU interpreting the powers of DPAs over data transfers out of the EEA in light of the need to ensure complete and effective protection of individuals. E.g *Schrems I:* "The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities." Para 41.
[941] Articles 78, 79 GDPR.
[942] C-40/17 *Fashion ID* (ECLI:EU:C:2019:629); C-61/19 *Orange Romania* (ECLI:EU:C:2020:901).

permitting processing accords with fundamental rights standards[944]) it is the courts and data protection authorities who make these determinations. The courts can act as a corrective or check upon national or EU legislative paternalistic measures, by striking down measures which purport to allow processing,[945] or can fill in detail in the broadly drafted principles of the GDPR.

Indeed, the CJEU in particular has taken on a significant law-making role in EU data protection law,[946] and in doing so have had considerable influence on the types of data processing which can occur. Bygrave and Schartum have pointed to the flexibility that the application of the proportionality principle can afford the courts (to engage in systemic considerations, including desirable levels of societal control of data).[947] To take one example, in *ASNEF,* the CJEU implicitly adds a criterion to the legitimate interests basis for processing data, by finding that in conducting the weighing assessment, that "the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources."[948] Processing of data in non-public sources is said to be a "more serious infringement" of the rights to respect for private life and data protection (arguably conflating these rights).[949] Thus, the CJEU determines that public data is to receive lesser weighting in a legitimate interests assessment, illustrating how the Court may intervene to influence the purposes for which data processing may be conducted, without regard to the individual data subject's choice or preference in this case.

In this way, we can see that much of the procedural apparatus created by EU data protection law to secure its own enforcement may be regarded as protective, as the individual's interests and rights are relevant to the final determinations, but protective in a paternalistic sense, as the individual has little autonomous input into such determinations. It is for the individual to plead for assistance, by way of initiating a legal complaint before a DPA or a judicial authority, but once begun, it is the public institution which has determinative power over the matter.

4.3. Structural paternalism

Just as we might say EU data protection law contributes to an environment which supports individual choice, in many areas, the law may be said to contribute to a paternalistic environment, in which such individual choice is supplanted by controller or public decision making.

One of the clearest ways in which we can see how the law upholds an environment in which the individual is not the primary decision maker over data processing practices is in the very concept of the "data controller". The controller is defined as the entity who "alone or jointly

---

[943] C-524/06 *Huber v Germany* [2008] ECR-I-09705.
[944] For example, Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238); C-201/14 *Bara and Others* (ECLI:EU:C:2015:638); C-398/15 *Manni* (ECLI:EU:C:2017:197); C-73/16 *Puškár* (ECLI:EU:C:2017:725).
[945] See discussion on the use of Article 8 as a basis for the assessment of the legality of EU and national legal measures, in Chapter 2, section 3.1.
[946] On the role of purposive interpretation and the transformative effect it has had on key threshold concepts of EU data protection law, see Chapter 2, section 2.2(a).
[947] Bygrave and Schartum (n 85) 167.
[948] Joined cases C-468/10 and C-469/10 *ASNEF* [2011] I-12181, para 44.
[949] ibid*,* para 45.

with others, determines the purposes and means of the processing of personal data".[950] Thus, the default notion is that controllers are decision makers, not the affected individuals.

In this definition is encapsulated a core idea, which permeates the law: that the controller is the decision making entity, and because of this power, it is held responsible for such data processing. As Van Alsenoy has written, the implicit assumption within the first generation of data protection laws was to target "data usage by resourceful public and private sector organisations" and such assumptions have been difficult to shift.[951] Further, he writes that "the concept of controller implies an exercise of decision making power as to whether and how the processing will take place."[952] We might therefore say that an assumption as to who determines how data will be used has been cemented in the regime through the definitional approach to the controller, and the choice to design the regime around a relationship between controllers and subjects. We can imagine alternative delineations of responsibility amongst actors, and indeed current movements aimed at the creation of data trusts, co-operatives and commons might be formulae for alternative approaches.[953] We could also imagine approaches which define responsibility based on particularly harmful data misuses rather than focusing on controller-subject relationships. But such approaches are not found within the law, rather the controller is both assumed to be and defined as the primary decision-maker of data protection law. The pre-supposition is that the controller is the entity which decides how and why data may be processed, and all such entities are captured and regulated by the GDPR. While they may at times be bound to consider the individual's wishes (to lawfully obtain consent, or fulfil a contract) and they must act within the constraints of the law, it is the controller who determines how and why data must be used and indeed it is their decisional autonomy which renders them a controller. While we might characterise this is a legislative reaction to existing social and economic practice, Cohen would remind us that the relationship between law and socio-technical systems is dynamic,[954] and the legal cementing of such a conception of the controller may have reinforced it societally and economically.

The principle of accountability reflects and draws upon this structural paternalism. Accountability as a principle in data protection law has had a variety of conceptions and existed since the 1980s at least,[955] and introduced to the GDPR in the desire to improve data protection compliance. As De Hert characterised it, the principle was to make organisations "more responsible".[956] Without delving into its effectiveness as a matter of compliance/enforcement strategy, we can see how the principle that controllers are bound be responsible for, and demonstrate compliance with the data protection principles,[957] and

---

[950] Article 4(7), GDPR.
[951] Van Alsenoy (n 83) 5–6. As Van Alsenoy has written elsewhere, at the time of the first national data protection laws, computers were rarely found outside universities, governments or large corporations, and even by the 1980s when Convention 108 was adopted, it was still the era of the centralised mainframe computing. Van Alsenoy (n 302) 27.
[952] Van Alsenoy (n 302) 31.
[953] For example see Delacroix and Lawrence (n 725); Wong, Henderson and Ball (n 725).
[954] Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (n 27) 8–9.
[955] See Denis Butin, Marcos Chicote and Daniel Le Métayer, 'Strong Accountability: Beyond Vague Promises', in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 343.
[956] Paul De Hert, 'Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan UK 2012).
[957] Article 5(2), GDPR

GDPR compliance more broadly,[958] reinforces an idea that the data controller is the primary decision maker over data usage.

In this way, we can say that the framing of the data controller as the decisional entity and the reinforcement of that framing through the principle of accountability suggests a structural paternalism. Decision making is primarily for controllers, not for individuals as data subjects.

5. Assessing the balance

In the foregoing sections of this chapter I have offered an account of the ways in which EU data protection law seeks to both empower and paternalistically protect the individual, in three senses: substantively (with regard to the purposes to which data may be used), procedurally (to defend an individual's legal interests and rights) and structurally (to create an environment within which the individual may be protected or empowered.) In this final section I consider the balance between these aspects of the law, and consider what picture of the individual emerges from this balance.

5.1. Paternalist protection versus empowerment of the individual

I have laid out above a framework of paternalistic protection and empowerment of the individual through the ideas of substantive, procedural and structural empowerment or paternalism within EU data protection law. I now move to consider the balance within these perspectives, before offering some thoughts on how this contributes in a more holistic sense to the balance between empowerment and paternalism overall.

The substantive framework of the law, which governs the purposes to which data may be put, I have located primarily in the legal bases for processing. In substantive terms, consent and contractual necessity as legal bases for data processing serve as the central means by which the law secures individual choices over data processing. When an individual consents to processing, or enters into a contract, these choices may serve as the basis for the controller to justify their processing. These bases are the strongest argument for an individual getting to choose *why* their data is processed, and yet are still relatively weak grounds to defend individual control. The controller is the one who gets to formulate the data processing proposal and the individual's choice is generally limited to whether or not to accept such a proposal. Moreover, a failure to consent or choose to enter a contract is not fatal to that data processing purpose. Rather, the controller can move on to seek to rely on an alternative ground. Thus an acquiescence is respected by the regime, but a refusal is not necessarily. The remaining legal bases are beyond the choices of the individual, and while their interest is not irrelevant to processing on the basis of vital interests, public interest, legal obligation, or legitimate interests, they are not an active participant in the determination of the purpose of processing. On a formal level, the predominant approach to the regulation of the purposes of data protection may be classified as a paternalistically protective approach. Individual empowerment is limited, and only guaranteed to be protected where they are a willing participant in the processing they are offered.

The procedural elements of the law are a similar mix of empowering and paternalistic elements. The rights to access and to portability can be important facilitative tools to support individual choice, by granting individuals legal rights to access information to aid decision making and to transfer their data to alternative service providers. The remaining individual data rights are not empowering in the sense of providing an individual with meaningful choice or control over their life, though they can be seen as important tools to safeguard

[958] Article 25, GDPR.

one's legal interests. The right to objection can provide an individual an opportunity to intercede to have their particular circumstances weighed in circumstances where it is a counterweight to other interests justifying data processing. The rights to rectification, erasure and restriction are largely defined in terms which links their operation to existing illegal processing by data controllers, and on this basis these rights might be classified as enforcement tools, to constrain illegal data processing, and while this might accord with a narrow conception of control, it would be a considerable stretch to consider such enforcement tools as meaningfully empowering data subjects. Indeed, requiring individuals to act in their own self-defence may be criticised as improper responsibilisation or burden.[959]

In a structural sense, the law makes some attempt at obliging controllers and legislators to have regard to individual's data choices, by mandating that they consider loss of control as a risk to be considered in the implementation of controllers' obligations and in legislative derogations. The paternalistic protective structure of the GDPR is implicit in the concept and role of the data controller, who is defined as the primary decision maker over data processing, a role which justifies holding them responsible for data processing, which is reinforced through the notion of accountability. In other words, it is the data controller's world, the data subject just lives in it.

After the weighing of these competing strategies to individual protection, we are left with an approach built on more paternalistic strategies than we might have expected based on the pervasive discussions of control of data and individual empowerment. Those provisions of EU data protection law which formally might be said to contribute to individual empowerment bear a closer relation to a narrow sense of control, such as Bygrave's conception of participation or "a measure of influence" over data processing,[960] but this falls short of individual empowerment in the sense of securing individual choice or self-determination. Of course, any legislative scheme which involves choice will include some form of paternalism (even an absolutist libertarian approach).[961] In this sense paternalistic approaches can restrict protections to the individual as other interests are incorporated and to be weighed against an individual's data protection interests, including the controller's legitimate interests and the rights and interests of other parties. And paternalism can operate to protect an individual's interest (as least from the viewpoint of the legislator), where protections are imposed in their name, but which have the effect of removing the individual from the decision making arena.[962]

As a result, we may say that EU data protection law is more paternalistic than perhaps is conventionally considered. The individual's interest and position in EU data protection law should therefore not be conflated with their decision making powers. While consent might have elevated significance through its position in Article 8 of the Charter and its conceptual link to informational self-determination, within the context of the wider GDPR framework, it is but one (relatively weak) form of empowerment, amongst many more paternalistic formulations.

---

[959] See Chapter 2, section 5.4.

[960] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 18) 87.

[961] As Sunstein has written, even relying upon active choice involves a form of paternalism, as some individuals could prefer not to choose, and yet they may be saddled with a responsibility for choice. Cass R Sunstein, 'Requiring Choice Is a Form of Paternalism' (2017) 1 Journal of Behavioral Economics for Policy 11, 11–12.

[962] For example, the principle of accountability is an example of a measure which aims to protect individuals through the attachment of compliance responsibility to controllers, but at the same time, it may be said to cement a controller's decisional role, rather than involve the individual in the decision making process regarding their data.

On the other hand, legally, paternalistic elements of the regime are doing much of the data protection "work", and yet there is no coherent conception apparent from the law of what a paternalistic strategy to safeguarding data protection might be.[963] Bygrave and Schartum would characterise such approaches as proportionality based approaches,[964] but such a characterisation is not borne out in recent CJEU practice. The concept of "complete and effective protection" of the individual, continually reiterated and used by the CJEU to support judicial reasoning,[965] is lacking in substance, and tends towards absolutism rather than proportionality, seeming to assume that ensuring that the data protection legislation applies to every data processing activity will lead to better protective outcomes.[966]

In the alternative to "control" or autonomy based approaches, the collection of paternalistic approaches do not cohere into an easily explainable strategy. The lack of a coherent conceptualisation of the right to data protection beyond self-determination becomes more pressing when we consider the widespread criticisms of individualised control based approaches to data protection, and we are left grasping for alternatives. As Thomas has written, "[t]he way we conceptualize a public law right is important… because extrapolating what is morally salient about it can answer further questions about what we owe one another in the private law context. Thus the concept of rights we use will determine our ability to translate public rights into the context of public relations."[967]

To some degree, the absence of a coherent framework for the paternalistic strategies employed in EU data protection law is not surprising, given the patchwork nature of the GDPR, deriving from a range of historical antecedents.[968] Legislators designing the Data Protection Directive and GDPR were not working in a vacuum, but borrowing from international instruments and national legislative traditions to privacy, private life and data protection, presumably in the assumption that existing approaches (to which many stakeholders had already adapted) would serve as a successful basis for a harmonised protective approach.[969] However, just as the socio-technical context of the 1970s was to shape the assumptions and conceptions as to who was the decision-maker over data processing,[970] assumptions about the law and regulatory strategies have also been inherited by and shaped the GDPR, which may go some way to explaining the division between empowering and paternalistic approaches seen in EU data protection law.

5.2. Conceiving of the individual and the law, empowerment and the marketplace

When questioning the balance between empowerment and protection, and particularly conceptual disagreement over their respective roles, we have to recall that the GDPR is a legislative instrument, adopted with particular goals in mind, and in particular to safeguard

---

[963] Notably, Dalla Corte argues that the essence of the right to data protection is not substantive but procedural – a sort of due process right, or "right to a rule". Lorenzo Dalla Corte, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data protection and privacy: Data protection and democracy* (Hart Publishing 2020).
[964] Bygrave and Schartum (n 85).
[965] As described in Mahieu, van Hoboken and Asghari (n 387).
[966] See discussion in Chapter 2, section 2.2(b) and 3.2(b).
[967] Jean Thomas, *Public Rights, Private Relations* (Oxford University Press 2015) 19.
[968] See Chapter 3.
[969] Moreover, legislators are made up of a variety of actors with different political and philosophical perspectives, and these conflicting perspectives also had to be negotiated in the development of EU data protection law.
[970] Discussed in section 4.2 above.

the right to data protection. Both Ausloos[971] and Lazaro and Le Metayer have highlighted the need to distinguish between the theory of the right to protection and the legislative implementation of that right or theory. In Lazaro and Le Metayer's words, there can be a "conflation between the *conceptualization* and *management* of privacy."[972] This chapter is concerned primarily with the implementation of the right to data protection (i.e. the *management* of data protection), and in particular how a right usually conceptualised as concerned with individual empowerment is translated into a legislative regime which balances empowerment and paternalistic approaches, with a balance towards paternalism. As a legislative project, the conceptualisation of the right to data protection may inform legislative design, but these conceptualisations become intertwined with other assumptions and conventions about regulatory practice and the role of law in order to draft a comprehensive piece of legislation. It would be impossible to consider all such shaping assumptions and conventions, and so in this section, I focus on one way in which the law's form manifests such assumptions. I consider how the types of choices respected or facilitated by EU data protection law reflect ideas of a public/private sector divide and a connected idea of market-mediated relationships as the primary site for individual empowerment.[973]

First, we recall that the empowerment of the individual under the GDPR derives from a series of key elements of the GDPR; consent and contractual necessity as a basis for data processing, the right to data portability (i.e. choice to move to another data controller), transparency obligations and the right to access as a facilitative informational tool. We remember that consent is deemed inappropriate for most public sector data processors, given the difficulties in establishing consent is "freely given" in such contexts.[974] Consent, and the closely related contractual necessity ground for processing, become more relevant in the context of private relationships, particularly market relationships, given the understanding of data as an economic asset which also pervades the GDPR.[975]

The notion that consent/contract is the primary basis for regulating private relationships is a long-standing convention in law. This has been connected to the idea that the market is the appropriate means for the mediating between private individuals. Horwitz connects these ideas to dominant 19th century legal thought, as the market emerged "as a central legitimating institution", critical to the historical emergence of the public/private distinction in legal discourse, and "private law came to be understood as a neutral system for facilitating voluntary market transactions and vindicating injuries to private rights."[976] Today, the

---

[971] Ausloos critiques those who fail to distinguish between the right to data protection (as protected by Article 8 of the Charter, which he conceives of control oriented) and data protection legislation, which seeks to achieve a fair balance between that right and other rights and interests. Ausloos (n 84) 73.

[972] Lazaro and Le Métayer (n 310) 15.

[973] While the public / private distinction is not without controversy, these broad categories of actors do seem to be reflected in the existing regime. On the controversy over this distinction see e.g. Carol Harlow, '"Public" and "Private" Law: Definition Without Distinction' (1980) 43 The Modern Law Review 241; Gerald Turkel, 'The Public/Private Distinction: Approaches to the Critique of Legal Ideology' (1988) 22 Law and Society Review 807.

[974] Recital 43, GDPR. 'Guidelines 05/2020 on Consent under Regulation 2016/679' (European Data Protection Board 2020) Version 1.1. 8–9 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 11 March 2023.

[975] See Chapter 3, section 4.2.

[976] Morton J Horwitz, 'The History of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1423, 1426.

ideological nature of this vision of private law has been recognised,[977] but we see a persistent reliance on market-based notions and strategies in the law.

In EU data protection law, many of elements of the legislative framework betray ideas of market conceptions. Indeed, the primary areas in which individual choices over data are to be respected by the GDPR are when those choices take the form of a market action. Thus, individuals may be empowered through the market, by freely consenting to engage with a data controller or entering into a contract. In this sense, when individuals engage with private sector data processors, this role for consent and contract echoes the familiar convention of legal theory that private actors are sustained by private law: particularly, contractual powers.[978]

EU data protection law does not defer unquestioningly to the market, of course, but often intervenes to protect data subjects. Still too, when the GDPR intervenes to protect the data subject in these cases, it is often reminiscent of the strategies applied to a consumer in an unfair bargaining position. When we look to the limitations on consent and individual choice, they often mirror an idea of the individual as a consumer engaged in a market-based transaction, and reflect consumer protective approaches; providing clear and intelligible information, and preventing "unfair" bargains. We see this in the requirements that a consent may be obtained in the form of a written declaration, but should not be bundled with other terms and conditions,[979] that data subjects should not be unfairly tied to providing data in return for the provision of a service.[980] Special rules are put in place for children, but primarily in the context of children who are in receipt of information society services.[981] Thus, while in these cases the GDPR does not rubber-stamp a free market exchange of data, it continues to reflect market logics in its legislative strategies. An inequality in bargaining power can be solved through consumer protection, fairer terms to bargains and improved decision making through providing clearer information. A data subject and a data controller are engaging in an exchange, one which is economically valuable and should be permitted to proceed, within constraints. The empowerment of the data subject is implicitly an empowerment to engage in economic transactions, to participate in the marketplace for personal data.

It is uncontroversial to say that EU data protection law balances marketplace and fundamental rights objectives,[982] however, when we look to how the fundamental right comes to be managed through the GDPR, it becomes clearer that the logic of the marketplace comes to inform how that fundamental right is to be protected. In this way, just as has been observed in other fields of regulation, the GDPR is "a product of dominant ideas and worldviews",[983] and allocations of risks and responsibilities can be influenced by assumptions as to the appropriate position of the market and of self-regulation.[984] Clearly, EU data protection law does not adhere to an ideology which completely absolves the private sector of scrutiny, but it does conceive of individual empowerment in terms of marketized transactions.

---

[977] ibid 1427.
[978] Thomas (n 967) 3.
[979] Article 7(2), GDPR.
[980] Article 7(4), GDPR.
[981] Article 8, GDPR.
[982] Article 1, GDPR. See also Lynskey (n 133).
[983] Martin Lodge and Kai Wegrich, *Managing Regulation* (Macmillan Education UK 2012) 36 <http://link.springer.com/10.1007/978-1-137-26552-4> accessed 7 January 2022.
[984] ibid 37–38.

When we come to see how individual empowerment has come to be associated with a marketized vision of empowerment, the limited ambitions of the law are revealed. EU data protection law does not attempt to disrupt the status quo, or shape a digital environment in which individuals have a real stake. Rather, individuals should have only “control” of their data, and only to the extent that they will sign up to the market offerings which are provided to them.

This might perhaps reinforce the need to re-examine the conceptualisation of paternalistic strategies to manage data protection, and the vision of how individuals are to be safeguarded in default of their own empowerment. When empowerment is conceived of narrowly, and often in marketized terms, and is subject to a considerable critical literature, increased pressure comes on alternatives to empowerment strategies. In the next chapter, we will see some of the ways this manifests when it comes to the impact of EU data protection law on differently situated persons, and how empowering and paternalistic strategies can contribute to differential protective standards.

CHAPTER 6: DIFFERENCE, UNIFORMITY AND THE INDIVIDUAL

1. Introduction

When we think of the data subject as an *individual,* this invites questions as to the type of individual or person envisaged. This chapter furthers our engagement with the conception of the individual data subject and asks, how are ideas of uniformity or diversity of the individual reflected in EU data protection law? Does the GDPR understand individuals to be diverse or uniform, and what are the consequences of these conceptions for the operation of the law? In Chapter 4, I examined the extent to which the GDPR conceives of the data subject as individuated versus relational, and in doing so, invoked a broader collective of data subjects, beyond the individual. In this chapter, I return to that collective, to once again examine the relationship between the individual and other data subjects, but with another question in mind. Is the individual data subject distinct or different from other data subjects? Or are all data subjects the same—uniform?

This debate over difference versus sameness, heterogeneity versus homogeneity, is also reflected in broader literature on legal personhood and subjectivity. Boyle points to this as an opposition between the universal and particular vision of subjectivity.[985] Moreover, the issue of difference between data subjects has received some attention. Blume, in his 2015 article "The data subject" was the first to question "whether data protection law should differentiate between different types of data subjects in order to achieve its main purpose."[986] At this stage, he notes that the GDPR singled out children for special treatment as data subjects.[987] Many scholars have pointed to the need for special rules or approaches to the data protection of children, for a variety of reasons.[988] A further category of special data subjects is suggested by the inclusion of the related concept of *vulnerable* data subjects within the GDPR, and the call for special approaches to such vulnerable data subjects, notably by Malgieri and Niklas.[989] In this way, the question of difference has arisen in order to interrogate whether the GDPR (or data protection law more broadly) is fit for purpose: if different types of data subjects exist, are they all adequately protected by the law?

My contribution seeks to link these literatures and questions it in a new fashion. First, rather than assuming the category of a data subject necessarily means a one-size-fits all approach, through an examination of how the abstracted "data subject" is understood and applies, I argue that EU data protection law can accommodate some degrees of difference between data subjects. This differentiation is seen through application of individualised standards and express recognition of some differences between data subjects. Nevertheless, not all types

---

[985] Boyle (n 17) 518.
[986] Blume (n 59).
[987] ibid.
[988] For example: Milda Macenaite, 'From Universal towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19 New Media & Society 765; Lievens and Verdoodt (n 244); Sonia Livingstone, 'Children: A Special Case for Privacy?' (2018) 46 Intermedia 18; Donovan (n 689).
[989] Malgieri and Niklas (n 244). See also Ryan Calo, 'Privacy, Vulnerability, and Affordance' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (1st edn, Cambridge University Press 2018) <https://www.cambridge.org/core/product/identifier/9781316831960%23CN-bp-11/type/book_part> accessed 27 January 2022; Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR When Vulnerable People Use Smart Devices' [2022] International Data Privacy Law ipac001.

of difference may be recognised or accommodated, and moreover, exclusionary assumptions about personhood are embedded in the law.

This is explored through three sections below. Section two introduces the existing literature and theoretical background on the issue of uniformity and difference of personhood. Section three considers three areas in which data protection framework operates around an archetypal legal person and the implications of such an approach for differently situated persons. Section four looks to those areas of the law which do recognise difference, and considers how special rules for specific types of data subjects operate to protect differently situated individuals.

2. Uniformity versus difference

If, in the words of Monty Python, "we are all individuals",[990] what makes an individual distinct from the common mass of humanity? The individuated person,[991] to be separate from the collective, must be distinguishable in some way, and thus the idea of difference may be connected to individuality. The ways in which individuals differ can be explored from endless perspectives, including embodiment, identity, experience or circumstance. Moreover, the law has sought to respond to such difference, and there is no consensus on how to secure justice or equality in the face of difference. The broader political and metaphysical debate is beyond the scope of this chapter, but a narrower question poses an interesting issue for EU data protection: does the existing model of legal personhood accommodate or allow for difference, or does it assume uniformity? If we can accept that difference exists between persons, without needing to agree on how to conceptualise such difference, we can question whether the law is able to accommodate or respect such difference. This becomes all the more pressing in light of heightened harms associated with surveillance of certain persons and communities.

2.1. Difference / pluralism in legal personhood

The notion of difference between subjects and the consequences of diversity of subjects has been developed in a variety of literature on legal personhood.

Scholarship on legal personhood often focuses on whether or not someone or something is a person within the meaning of the law, and thereby attracting its protections. Accordingly, we see works on whether or not foetuses, animals, artificially intelligent robots or even natural features such as rivers should be protected as a type of a legal person.[992] Thus

---

[990] Jones, Terry. *The Life Of Brian*. United Kingdom: Python (Monty) Pictures, 1979.

[991] See also Chapter 4.

[992] For example: Jane ES Fortin, 'Legal Protection for the Unborn Child' (1988) 51 The Modern Law Review 54; Stephen M Wise, 'Legal Personhood and the Nonhuman Rights Project' (2010) 17 Animal Law 1; Andrea Mulligan, 'Maternal Brain Death and Legal Protection of the Foetus in Ireland' (2015) 15 Medical Law International 182; Paul Waldau, 'Animals as Legal Subjects' in Linda Kalof (ed), Paul Waldau, *The Oxford Handbook of Animal Studies* (Oxford University Press 2017) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199927142.001.0001/oxfordhb-9780199927142-e-13> accessed 13 May 2022; Lisette ten Haaf, 'Unborn and Future Children as New Legal Subjects: An Evaluation of Two Subject-Oriented Approaches—The Subject of Rights and the Subject of Interests' (2017) 18 German Law Journal 1091; Aikaterini Argyrou and Harry Hummels, 'Legal Personality and Economic Livelihood of the Whanganui River: A Call for Community Entrepreneurship' (2019) 44 Water International 752; Simon Chesterman, 'Artificial Intelligence and the Limits of Legal Personality' (2020) 69 International and Comparative Law Quarterly 819; Sylwia Wojtczak, 'Endowing Artificial Intelligence with Legal Subjectivity' (2022) 37 AI & Society 205.See also the collected discussions in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer 2017).

already, within the fiction of the legal subject can be accommodated different types of "persons". However, alongside the question of status of non-human subjects as persons, there is also literature which considers the qualities of the human legal subject, or the type of person who is presupposed by the legal regime. Some such qualities have been considered in previous chapters.[993]

One lens through which legal personhood has been explored is the question of difference, or pluralism. Sometimes the nature of the difference is the focus of the study, often in the context of rights or constitutional protections. For instance, feminist scholars have questioned the gendered nature of the legal person.[994] Theorists also have interrogated legal personhood and individual rights on the basis of race[995] and disability.[996] Beyond specific difference, others have questioned how difference in general has come to be significant in the construction of legal personhood. Often this is considered in reference to anti-discrimination laws. To take one example, in the context of US anti-discrimination laws, Kirkland has argued that difference has come to be debated and then recognised in law due to "logics of personhood", which are "ways we explain to each other how and why someone's traits should or should not matter for judging what is really important about her".[997] In other words, difference becomes significant in Kirkland's study when it confers legal status. As we shall see, some differences do confer additional legal protection in the data protection regime. Further, some differences become relevant because of their effective exclusion from the data protection regime.

2.2. Different experiences of data processing and surveillance and the 'model' data subject

Difference is relevant to an investigation of personhood and the conception of the individual in data protection law for a number of reasons.

First, the experience of data processing and surveillance is not even. Marginalised populations are disproportionately surveilled and often have less power to resist data misuse than others.[998] Harms associated with data misuse can thus exacerbate existing inequalities

---

[993] On the subject as market participant, see Chapter 3 and 5, and on the subject as a relational or individuated person, see Chapter 4.

[994] For example, Naffine has argued that the patriarchal history of the concept of the legal person must be wrestled with in the same manner as positive legal instruments have been scrutinised for sexist impact. Naffine (n 16).

[995] For example, see Patricia J Williams, 'Alchemical Notes: Reconstructing Ideals from Deconstructed Rights' (1987) 22 Harvard Civil Rights-Civil Liberties Law Review, 401; Patricia J Williams, *The Alchemy of Race and Rights* (Harvard University Press 1991); Neil Gotanda, 'A Critique of "Our Constitution Is Color-Blind"' (1991) 44 Stanford Law Review 1; Kimberle Williams Crenshaw, 'Race, Reform, and Retrenchment: Transformation and Legitimation in Antidiscrimination Law' (2011) 12 German Law Journal 247; Leti Volpp, 'The Citizen and the Terrorist' in Cyra Akila Choudhury and Khaled A Beydoun (eds), *Islamophobia and the Law* (1st edn, Cambridge University Press 2020) <https://www.cambridge.org/core/product/identifier/9781108380768%23CN-bp-1/type/book_part> accessed 21 February 2023.

[996] Fiona AK Campbell, '"Disability's" Date with Ontology and the Ableist Body of the Law' (2001) 10 Griffith Law Review 42; Ingunn Moser, 'Disability and the Promises of Technology: Technology, Subjectivity and Embodiment within an Order of the Normal' (2006) 9 Information, Communication & Society 373; Margrit Shildrick, *Dangerous Discourses of Disability, Subjectivity and Sexuality* (Palgrave Macmillan 2009).

[997] Anna Rutherford Kirkland, *Fat Rights: Dilemmas of Difference and Personhood* (New York University Press 2008) 2.

[998] In surveillance studies, rather than assuming that there is a common homogenous impact or experience of surveillance, many scholars engage with a diversity of individual and group experience of surveillance. The difference in capability to resist surveillance is a common theme in surveillance scholarship. For example, McCahill and Finn engaged in an extensive empirical study in a northern

and societal oppression. In this chapter, I argue that this is recognised to a small degree in the regime, and is the implicit rationale behind some provisions of the law, but in a piecemeal rather than holistic sense.[999] The different experience of data protection has been located by some scholars recently in the concept of vulnerability. Notable recent scholarly attention to the notion of vulnerable data subjects[1000] is seen in the works of Malgieri and Niklas[1001] and Piasecki and Chen.[1002] This nascent literature on vulnerability is interesting for a couple of reasons. It illustrates how scholars are beginning to grapple with the idea of diverse populations and how their needs might be accommodated within EU data protection, though at this early stage there is an understandable lack of specificity in both the problematisation and the proposed responses to vulnerable data subjects. Moreover, it is interesting from the perspective of difference, as vulnerability is being used as a framework to assess diversity of data subjects. Given the particularities of the conception of notion of vulnerability is beyond the scope of this chapter,[1003] and the sufficiency of the broader concept of difference to my enquiry, I do not propose to adopt this analytical tool in my study. Where relevant, I note points of intersection in this chapter between the idea of difference and vulnerability.

Second, this understanding of difference of personhood comes into tension with the "model" data subject which informs the logic of EU data protection law. The GDPR is premised upon an archetypal individual data subject, and operates around this model legal subject. Blume criticised this element of EU data protection law, writing "[d]ata subjects are not a homogenous group of people and it is possible to make distinctions with respect to their position and status under protection law" and advocated for amendment of the existing regime to account for such difference.[1004] As I shall explore, however, the law does allow for some differentiation in practice and therefore the "model" may not be quite so rigid as Blume complained.

3. The data subject: generalised in framing, differentiated in practice

One concern which may arise with a generalised or archetypal legal person is that the legal model of personhood may not be representative of all the pluralistic population who ought to

---

UK city in order to study a series of different groups and their experience of surveillance (including journalists, school children from different economic backgrounds, protestors, migrants, criminal offenders), and a significant differential impact amongst such groups, and concluded that "[t]he ability to mobilize social, economic and cultural capital to evade or contest surveillance is not equally shared.". McCahill and Finn (n 791) 178. See further David Barnard-Wills, *Surveillance and Identity: Discourse, Subjectivity and the State* (Ashgate Publishing Ltd 2012); Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge University Press 2021).

[999] See section 4, below.

[1000] The concepts of privacy and vulnerability have received some earlier attention by US scholars. Khiara Bridges, 'Privacy Rights and Public Families' (2011) 34 Harvard Journal of Law and Gender 113; Calo (n 989).

[1001] Malgieri and Niklas have advocated for the adoption of the vulnerability concept to address the needs of vulnerable data subjects through reinterpretation and enforcement of the GDPR. Malgieri and Niklas (n 244).

[1002] Piasecki and Chen have taken Malgieri and Niklas's suggestion to consider difference and examined the application of the GDPR to the use of smart devices which are used by vulnerable people. Piasecki and Chen (n 989).

[1003] The conception of vulnerability is contested, multi-layered and intertwines normative and ontological claims which are not necessary to resolve a simpler but no less relevant question: that of difference. The existing literature illustrates a struggle to identify the source of vulnerability, or substantiating the affected subjects. Malgieri and Niklas acknowledge the challenges of the vagueness and instability of the vulnerability concept. Malgieri and Niklas (n 244) 4.

[1004] Blume (n 59) 259.

be protected through the legislation premised on this model. For example, in Barnard-Wills' study of public discourse on surveillance, he identifies certain assumptions about the type of individual who experiences surveillance: "a particular model of the individual (educated, property owning, in relationships with banks and financial institutions, with a respected and non-tarnished identity, and identifying primarily as an individual rather than a member of a collective) is used as a universal model applicable to all individuals."[1005] What do such assumptions mean for those who fall outside this model? If the law is premised upon a similar model of a person, against the recognition that personhood is diverse, we may question whether all data subjects are protected in the same way, or whether the archetypal model is sufficiently flexible to differentiate between individual experience in practice? This was a concern which informed Blume's critique, discussed above.[1006] With this question in mind, this section examines how the law's model of the data subject operates. Through a doctrinal examination of the relevant legislation and case law, I argue that the regime finds a balance between a generalised legal framing and individualised differentiation.

While this is not a question which has been expressly considered by the Court or mentioned in the legislation,[1007] there is evidence in the decisions of the CJEU of an implicit awareness of this issue. Therefore my enquiry has been an inductive one, guided by the case law which has at least some evidence of grappling with this question. On this basis of this examination, in a number of discrete areas, a pattern emerges. In considering individually defined obligations, in the case law on the transparency obligations upon data controllers, the Court balances general and specific individualised framing of those obligations. Regarding individually exercisable data subject rights, the Court has also begun to consider how specific and individualised responses to requests must be. In its decisions regarding collective representative actions, we see early indications of how the Court understands such collectives to be formed, and a willingness to proceed on the basis of a hypothetical represented data subject.

3.1. Individually defined obligations: transparency notices

Many of the obligations upon controllers are defined in terms of the individual,[1008] and in this framing, the archetypal data subject is invoked. One such example is the transparency obligation placed upon the data controller,[1009] and in the interpretation of this obligation, we can see one way in which such individually defined obligations can accommodate difference, through a balance struck between generalised and particular application of these provisions.

As with many of the obligations under the GDPR, these obligations are expressed in relation to the singular notional data subject. Information is to be provided, "to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[1010] The importance of the transparency obligation has been linked to the data subject's capacity to exercise their data

[1005] Barnard-Wills (n 998) 135.
[1006] Blume (n 59).
[1007] With the exception of a singular mention of "vulnerable data subjects", considered further in section 4.2 below.
[1008] For this reason, I have argued the individual serves as the central subject of data protection law, see Chapter 2, section 3.
[1009] Articles 12-14, GDPR.
[1010] Article 12(1), GDPR.

rights,[1011] to the principle of 'fair processing'[1012] and to the fundamental rights of data protection, respect for private life and to an effective remedy.[1013]

The balance between the general and the particular data subject has special practical significance in the context of transparency notices. After all, most data controllers adopt a single generalised policy or set of policies, rather than tailored or individualised policies, for convenience. Thus, the notional model data subject takes on significance, as the legality of the transparency notice pragmatically has to be framed in terms of this notional data subject.

We see such an approach in the opinion of Advocate General Spzunar in *Planet49,* wherein he elaborates the informational standards upon data controllers.[1014] In order to determine the nature of information to be provided, Spzunar looks to an objective standard:

> *Given the conceptual proximity of an internet user (and provider) to that of a consumer and trader), one can resort at this stage to the concept of the average European consumer who is reasonably well informed and reasonably observant and circumspect and who is able to take the decision to make an informed commitment.*[1015]

Thus, the fiction of the notional data subject is crystallised: controllers are to have regard to an average consumer in designing transparency notices.

The Court does not endorse the use of the average consumer test, and rather focuses on the specifics of the information to be provided in relation to cookie usage, though it does implicitly adopt a vision of the nature of an affected data subject, finding that "clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed."[1016]

Nevertheless, this is not to say no regard is had for particular data subjects who might not be adequately informed by such a generalised notice. We do see a few instances of the Court

---

[1011] For example, in C-201/14 *Bara and Others* (ECLI:EU:C:2015:638), para 33: "the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive."

[1012] ibid, para 34: "the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of those data."

[1013] In Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656): the CJEU considered the individual rights of air passengers, and with regard to data protection emphasised that Article 8(2) of the Charter guarantees the rights to access and rectification, that the right to respect for private life "means that the person concerned may be certain that his personal data are processed in a correct and lawful manner. In order to carry out the necessary checks, that person must have a right of access to the data relating to him." (paras 218-219). And further, the Court determined that "In order to ensure that those rights are complied with, air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement. That information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal." (para 220).

[1014] C-673/17 *Planet49* Opinion of Advocate General Szpunar 21 March 2019 (ECLI:EU:C:2019:246).

[1015] ibid, para 113.

[1016] C-673/17 *Planet49* (ECLI:EU:C:2019:801), para 74.

grappling with the distinction between generalised and specific notifications. Interestingly, the Opinion of Advocate General Cruz Villalón in the *Bara* case suggests that a collective/generalised form of notice is the default, when he acknowledges that the affected data subjects "were not formally or individually notified" by the relevant data controller of the data transfer in question.[1017] Yet, we see that in this particular case, the Advocate General indicates that "a specific notification" of the data transmission was warranted."[1018] In Opinion 1/15, the CJEU determines that the informational provisions were insufficient, finding that "the general information provided to air passengers under Article 11 of the envisaged agreement does not afford them the possibility of knowing whether their data has been used … for more than those checks. Consequently, in the situations… in which there is objective evidence justifying such use … it is necessary to notify air passengers individually."[1019] In both cases, the attention seemed to be on a particular data usage, which because of its impact on a given individual, requires specific individual information to be provided.

In this way, we can see that in its application, the GDPR's transparency provisions, even if premised upon this archetypal data subject, do not stop there. If such a generalised notice does not address individual circumstance, further action must be taken by the data controller. Thus, while infrequently addressed by the Court, generalised practices which might be often adopted by data controllers are still judged by individualised standards. And because of this individualised approach, we can hope that transparency approaches might be more protective of a pluralistic population of data subjects, where supplemental individual notification or protection is warranted.

Nevertheless, we cannot say that all manner of data subjects are protected by this requirement of an individualised supplemental notifications. This concern arises because of the assumptions within the legislation itself about the function of transparency notices and the nature of data subjects. We have seen above that the Court has some notion that that the transparency obligation "implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed."[1020] Advocate General Spzunar gives us an indication of who an "average" user might be:

> *Thus, clear and comprehensive information implies that a user is in a position to be able to easily determine the consequences of any consent he might give. To that end he must be able to assess the effects of his actions. The information given must be clearly comprehensible and not be subject to ambiguity or interpretation. It must be sufficiently detailed so as to enable the user to comprehend the functioning of the cookies actually resorted to.*[1021]

In both of these formulations (and indeed in the underlying Articles of the GDPR) a series of assumptions are made about the nature of the data subject. As Blume has observed "[s]everal important parts of data protection law presuppose"…"the ability of the data subject to act as a data subject."[1022] The data subject is presumed to be able to read and comprehend information notices (provided it is in clear and plain language).[1023] The data

---

[1017] See C-201/14 *Bara and others* Opinion of Advocate General Cruz Villalón 9 July 2015 (ECLI:EU:C:2015:461), para 75.
[1018] ibid, para 79.
[1019] Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656), par 223.
[1020] C-673/17 *Planet49* (ECLI:EU:C:2019:801), para 74.
[1021] ibid, para 115.
[1022] Blume (n 59) 260.
[1023] Articles 12-13, GDPR.

subject is presumed to have sufficient decisional capacity and time available to use such notices to inform decision making about data choices and the exercise of rights and remedies. Differences of capacity are only recognised insofar as children are afforded particular protection.[1024] These provisions thus does not acknowledge or consider those who because of circumstance or disability may have literacy, learning or cognitive differences which limit their capacity to understand or act upon controller disclosures. Nor are the circumstantial or resource differences between data subjects considered, which mean that some persons have greater demands on their time or attention which limit their capacity to engage in data protection decision making. Given the criticism that data protection and privacy laws have faced to date based on even an "average" individual's capacity to act on their own behalf,[1025] effectively, without supportive structures this functions to exclude some individuals from any sense of data protection empowerment.

3.2. Individually exercised rights: data subject rights

This balancing between a generalised model and differentiated application of the law also arises in cases which consider data subject rights.

A key aspect of the data subject's rights is the idea that these rights are individually exercised and on the basis of an individuated notion of the data subject, as I have demonstrated in previous chapters.[1026] A corollary to such individual exercise is a case-by-case application and determination of these rights. In theory, therefore, we would expect a differentiation in application which can accommodate at least some differently situated data subjects. Indeed, there is some evidence for a differentiation in practice in the case law on the individual rights of access and right to be forgotten/erasure.

The right of access, often emphasised as the most important individual data right,[1027] is necessarily individually specific, as it grants the data subject a right of access to "personal data concerning him or her".[1028] Thus, we see in *Nowak* the CJEU constructing a test to determine which data in particular "relates to" a given data subject, determining this requirement to be satisfied "where the information, by reason of its content, purpose or effect, is linked to a particular person."[1029] Therefore, the right inherently operates on an individualised basis, as the practical response to a request for access must be tailored to the requesting data subject.

An interesting example of differentiation in practice is seen in the recent case of *RW v Österreichische Post AG.*[1030] This referral calls into question the interpretation of Article 15(1)(c) and the extent of the obligation to inform data subjects on recipients to whom personal data will be disclosed. In particular, the question goes to whether the data subject

---

[1024] Article 12(1), GDPR.
[1025] See Chapter 2, section 5.4.
[1026] See Chapter 2, section 4; Chapter 4, sections 3 and 4.
[1027] For example 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"' [2015] International Data Privacy Law ipv026; Xavier L'Hoiry and Clive Norris, 'The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, vol 34 (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-47573-8> accessed 21 June 2022; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4; Mahieu (n 84).
[1028] Article 15(1), GDPR.
[1029] C-434/16 *Nowak* (ECLI:EU:C:2017:994), para 35.
[1030] C-154/21 *RW v Österreichische Post AG* (ECLI:EU:C:2023:3).

is entitled to know *specific* data controllers to whom data is disclosed or mere categories of recipients. The Advocate General emphasised the purposive interpretation to be applied,[1031] and goes on to emphasise that Article 15 is a right of access attaching to the individual data subject: "Logically, the exercise of that right of access by the data subject presupposes that the holder of that right should be allowed to decide whether to obtain access to information concerning, where possible, the specific recipients to whom the data have been or are to be disclosed or, alternatively, to confine himself or herself to requesting information regarding categories of recipient."[1032] Looking to the purpose of the right of access in allowing data subjects to verify the accuracy and legality of processing, "implies that the information provided must be as precise as possible."[1033] This recommendation was endorsed by the CJEU, which echoes that the right of access "must be as precise as possible," and in light of the objective of ensuring a high level of protection of natural persons, "that the data subject has the right to obtain from the controller information about the specific recipients to whom the personal data concerning him or her have been or will be disclosed" except where if it is impossible to disclose such identity.[1034] This reinforces, as with the transparency cases discussed above, the assessment of compliance with the GDPR's provision is determined on an individualised basis, in accordance with a data subject's particular circumstances – in this case, specific information according to their preference.

The same tailoring to individual circumstance is clearly seen in the case law relating to the "right to be forgotten". In *Google Spain,* while the right comes to be framed by the facts of Costeja González's complaint, there is clearly an understanding by the CJEU of other types of data subjects who may seek to use the right, such as public figures, as the Court expressly has in mind a case-by-case rule. We see this as the Court considers the appropriate balance of rights between private life and data protection, the economic interest of search engine, and public interest in receiving information. As the Court finds that respect for private life and data protection generally override these competing interests, "that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."[1035] Again, an individualised rule is being adopted, to be tailored to the circumstances of the affected data subject. This is confirmed in the subsequent right to be forgotten cases, as the Court emphasises both the case-by-case nature of the right,[1036] and the relevance of the particular data subject's life and circumstances to that determination.[1037]

[1031] In light of the Charter rights, and to ensure the effectiveness of the provision. C-154/21 *RW v Österreichische Post AG* Opinion of Advocate General Pitruzzella 9 June 2022 (ECLI:EU:C:2022:452), paras 17-19.

[1032] ibid, para 21. Interestingly, the Advocate General contrasts this to the information obligations under Articles 13 and 14, because these are addressed to the controllers.

[1033] ibid, para 26.

[1034] C-154.21 *RW v Österreichische Post AG* (ECLI:EU:C:2023:3), paras 43-48.

[1035] C-131/12 *Google Spain and Google* (ECLI:EU:2014:317), para 97.

[1036] In *GC*, we see the Court finding that even where data has been manifestly made public, CJEU emphasises that data subject may still "have the right to de-referencing of the link in question on grounds relating to his or her particular situation." C-136/17 *GC and Others* (ECLI:EU:C:2019:773), para 65.

[1037] In *GC*, in finding the balance between respect for private life, data protection and freedom of information of internet users, "that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life." C-136/17 *GC and Others* (ECLI:EU:C:2019:773), para 66. In

From the right of access and right to be forgotten case law we can extrapolate to the broader class of data subject rights under the GDPR: these are (usually) individually exercisable, and compliance with these obligations (and sometimes the extent of the obligations) are judged by reference to the individual circumstances of the relevant data subject.[1038] In theory, therefore, difference between data subjects should be immaterial—each case and each data subject is to be treated in accordance with their circumstances.

Of course, as with the individually defined obligations under the GDPR, certain presumptions are made as to individual capacity to exercise these rights, which may have the effect of underserving or further marginalising certain subjects. The data subject is presumed to have the time and capacity to exercise individual rights where concerned about data misuse. Interestingly, in a recent Advocate General Opinion, the means by which a right to be forgotten claim was to be made against a search engine were questioned, and the Advocate General acknowledged the challenges individuals might face in bringing such requests.[1039] In weighing various procedural options, mere unilateral requests by data subjects are said to take too great a risk to the public's right to be informed, while a simple application request to the web publisher is said to be too blunt (the data subject is left without recourse in case of refusal), and an obligation to take a legal action against a web publisher deemed "a disproportionate sacrifice of the rights laid down in Articles 7 and 8 of the Charter."[1040] While the Advocate General emphasises practical difficulties which don't relate to individual identity (such as geographic obstacles or difficulties identifying the web publisher), an acknowledgement that legal action may be practically difficult, is interesting in light of the wider enforcement regime under EU data protection law. The CJEU follows this suggestion, and in determining the obligation of the data subject to establish the nature of the data inaccuracy, the Court seeks to "avoid imposing on that person an excessive burden which is liable to undermine the practical effect of the right to de-referencing."[1041] This indication—that inadequate procedural or other remedies within EU data protection law might incur a rights violation—could be a new lens through which to consider those data subjects who might be unable to avail of the GDPR's procedural rights, where the GDPR's individualised approach allows for insufficient recourse due to exclusionary assumptions.

3.3. Collective approaches and individualised implications: Judicial remedies

The preceding sections considered examples where the law is defined in terms of the individual—but what about those aspects of EU data protection law which do not expressly invoke the individual, or which seek to balance the individual with some wider collective? There is one area in which the Court has hinted to how such provisions might operate, which give us an indication of how differently situated individuals might be affected by such provisions.

TU, RE v Google, the CJEU emphasises the variety of specific criteria which must be weighed in striking a balance between freedom of expression, data protection and respect for private life, including "the degree of notoriety of the person affected… the prior conduct of the person concerned", again suggesting an individualised assessment is appropriate. C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962), para 60.

[1038] The right to rectification and right to erasure relate to "personal data concerning him or her" (Article 16, 17 GDPR), the right to objection is to be based "on grounds relating to his or her particular situation" (Article 21 GDPR).

[1039] C-460/20 *TU, RE v Google* Opinion of Advocate General Pitruzzella 9 June 2022 (ECLI:EU:C:2022:271).

[1040] ibid, paras 28-30.

[1041] Case C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962), para 68.

Collective representative actions by non-for-profit entities are created in two forms under the GDPR: those under Article 80(1) which are founded on an individual mandate,[1042] and those under Article 80(2) which are pursued independently of individual mandate, but because of infringement of a data subject's rights.[1043] Thus these provisions of the GDPR operate a type of balance between the collective or general vision of the GDPR's protective intent, while still being tied to the individual data subject, though perhaps a less individuated data subject than is suggested by other aspects of the GDPR.[1044]

These provisions came to be interpreted by the Court in the case of *Meta Platforms Ireland,*[1045] and the interpretation gives us some interesting indications of how the Court understands the relationship between the individual data subject and collective action, and in particular the level of individual specificity which is necessary to bring such actions.

The case concerned "whether [a consumer protection association] may bring proceedings against [Meta Platforms Ireland] in the absence of a mandate granted to it for that purpose and independently of the infringement of specific rights of the data subjects."[1046] Without such a mandate, the Court considered the case in light of Article 80(2), and whether this Article would preclude German national legislation which permitted a consumer protection association to bring action without individual mandate, in light of alleged infringement of the prohibition of unfair commercial practices, consumer protection legislation or the prohibition of the use of invalid general terms and conditions."[1047] In particular, the question arose as to whether specific individuals must be identified before such an action could be brought. The Court rejected this, finding that no "prior individual identification of the person specifically concerned" was required.[1048] Rather, the Court expressly approves of approaches based on notional data subjects is sufficient, finding that

> *the concept of 'data subject'… covers not only an 'identified natural subject, but also an 'identifiable natural person' namely a natural person 'who can be identified', directly or indirectly…. In those circumstances, the designation of a category or group of persons affected by such treatment may also be sufficient for the purpose of bringing such representative action*.[1049]

This approach is justified by the Court as consistent with the objective of ensuring high level of protection of the right to data protection,[1050] and the Court asserts that representative actions "undoubtedly contribut[e] to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection."[1051] This is grounded in the idea that representative action "could prove more effective than the action that a single person individually and specifically affected by an infringement".[1052]

[1042] Article 80(1) GDPR allows for such entities to lodge complaints or judicial actions on behalf of data subjects who have mandated that NGO.
[1043] Article 80(2) GDPR allows for complaints or judicial actions "independently of a data subject's mandate", if the relevant NGO "considers that the rights of a data subject … have been infringed as a result of the processing."
[1044] See Chapter 4.
[1045] C-319/20 *Meta Platforms Ireland* (ECLI:EU:C:2022:322).
[1046] ibid, para 48.
[1047] ibid, para 51.
[1048] ibid, para 68.
[1049] ibid, para 69.
[1050] ibid, para 73.
[1051] ibid, para 74.
[1052] ibid, para 75.

This approach is significant for a number of reasons, but in particular, I draw on it for two reasons. First, the Court's approach suggests something interesting about the nature of the "collective" which may be protected by an Article 80(2) action. That collective is one in which the data subjects can lose their individuality, as they are subsumed into a category or group. Perhaps, some degree of aggregation or homogenisation is inevitable in order to feasibly make a common action, but it does risk under-representing data subjects who fall outside the average. Those who are most at risk, face different harms associated with data use or those least able to engage in their own self-defence may be underserved by abstracted notions of data subjectivity.

Second, because of this process of abstraction, the Court may be unintentionally contributing to a particular balance of power in such cases. The representative NGO acquires particular strategic status: it may select its actions based on impact upon a notional data subject or category of data subject. NGOs thus have the power to shape the claim upon which the representative complaint or action is brought—and the data subjects who are to be protected. The risk arises again, that persons who are less visible, represented or advocated for in society might not be foremost in chosen strategic action. Some NGOs have historically been important defenders of minority interests in the privacy sphere, and this is to be welcomed, but there may be a question for the privacy and data protection community in ensuring that a broad range of the population is engaged as stakeholders in developing strategic priorities.

This is only the Court's first word on collectives of data subjects, and thus whether we can fully extrapolate from its decisions is yet to be seen. Nevertheless, it points to a number of interesting insights on the starting point from which collectives might be understood within the EU data protection framework and some consequences of such an understanding. If collective actions may arise by specific individual mandate or in order to protect a notional affected data subject, there is a significant risk that well-resourced individuals or those of "average" situation in society may be privileged in such representative action. This places particular importance on the prioritisation and choices made by NGOs, particularly those acting without data subject mandate, to ensure that those out of the mainstream are not excluded and highlights the special responsibility that NGOs have to support a broad population of data subjects.

3.4. Accommodating difference in application

From these initial areas, we can begin to extrapolate to other areas of the GDPR which mirror these provisions.

First, in areas where the relevant provision is framed around application to an individual data subject, differentiation is possible in practice. We might expect that as with the CJEU's instruction on the application of the transparency rules, if a generalised approach is insufficient in a given individual's circumstances, the controller is under an obligation to take further specific steps. Blume had considered this possibility in the context of fairness analyses,[1053] but I suggest in principle it could go much further—in principle to all those provisions which are defined in terms of the individual.[1054] We see this reinforced in the approach taken to data subject rights, where responses are expected to be precise and targeted to a given individual's data. This also raises the important safeguarding role that the rights to respect for private life and to data protection may have to allow individuals to assert

[1053] Blume (n 59).
[1054] See Chapter 2, section 3.

their particular circumstances. Thus, even where the law does not explicitly acknowledge difference between data subjects, the advantage of its individualist aspects may be in their application on a one-to-one basis, such provisions have to be tailored and accommodated to the individual data subject in question.

Yet, throughout, even where some degree of difference may be accommodated, there are assumptions about personhood baked into EU data protection law and the Court's interpretation of the law which operate to exclude or marginalise some subjects, particularly those who might require further support or be unable to act on their own behalf in the exercise of decision making or in seeking redress. The Court's acceptance of the use of "notional" data subjects in representational actions also risks further exclusion or omission in the purported representation of data subjects, highlighting the important responsibility of NGOs in this space. Of course, the GDPR does step in to provide additional special protection for a limited class of individuals, as we shall see in the following section, the question of course remains whether such additional special protection adequately captures the diversity of data subjects.

4. Express recognition of difference within the GDPR

Alongside the differentiation which is possible where individualised approaches are seen within the GDPR, we also can point to areas where the law expressly recognises certain types of difference, and particular categories of data subjects. In this section, I demonstrate that special categories of data recognised (i.e. sensitive personal data) align with some differences of identity between data subjects and that children and other vulnerable data subjects attract particular protection under the GDPR. What emerges, is a patchwork understanding of difference, but perhaps some sense of the types of difference which have been historically associated and legally recognised as raising additional harms in data processing.

4.1. Differences of identity: special categories of data

The clearest recognition of difference between data subjects is seen in the special protection which attaches to "special categories of personal data", also commonly referred to as "sensitive personal data". Article 9 of the GDPR imposes a prohibition without additional legal basis for the processing of:

> *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.[1055]

Such data are said to merit additional protection because they are "by their nature, particularly sensitive in relation to fundamental rights and freedoms" and "their processing could create significant risks to the fundamental rights and freedoms."[1056] This broad formulation of the heightened sensitivity of such data was echoed by the CJEU in *GC and Others* and *OT.*[1057] Notably in *GC,* the Advocate General had advocated for a more limited

[1055] Article 9(1), GDPR.
[1056] Recital 51, GDPR.
[1057] C-136/17 *GC and Others* (ECLI:EU:C:2019:773); para 44; Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601) para 126. The ECtHR have also taken into account the sensitive nature of special categories of data in many of its decisions under Article 8 of the ECHR. See e.g. *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997) (data concerning health,

interpretation of the prohibition on processing of special categories of data, to take into account "the responsibilities, powers and capabilities of an operator of a search engine."[1058] The CJEU rejected this interpretative approach, and rather found that a single standard of interpretation was relevant "to every kind of processing of the special categories of data referred to in those provisions and to all controllers carrying out such processing,"[1059] with a search engine responsible "in the same way as any other controller" to comply with the GDPR.[1060] The CJEU took its customary purposive interpretative approach, in this case in light of the sensitive nature of special categories of data, thus a limited interpretation of the prohibition "would run counter to the purpose of those provisions, namely to ensure enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute… a particularly serious interference with the fundamental rights to privacy and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter."[1061] Heightened scrutiny is warranted because "where the processing relates to the special categories of data … the interference with the data subject's fundamental rights to privacy and protection of personal data is… liable to be particularly serious because of the sensitivity of those data."[1062] In *OT,* a very similar pattern of reasoning led to the finding that data which allowed for an inference of sexual orientation (lists of spouses and partners by names) should also be classed as falling with Article 9 of the GDPR.[1063]

As Van Bekkum and Zuiderveen Borgesius have written, at least part of the rationale for designating special categories of data can be seen in a desire to prevent unfair discrimination, as the Council of Europe cited such a risk in the 1970s while developing early data protection standards.[1064] Nevertheless, as they write, while there is overlap, the categories of data attracting special protection are not exactly the same as those which are protected characteristics under anti-discrimination law.[1065] Georgieva and Kuner link the categories to anti-discrimination and to "[t]he history of Europe in the twentieth century" showing that sensitive data misuse "can facilitate human rights abuses on a large scale".[1066]

At their core, then, the special categories of personal data can be said to recognise that difference between individuals can be a powerful source of discrimination, hatred and harm. Some of the categories of sensitive personal data have some overlap with identity based characteristics of individuals which have been historically oppressed—racial or ethnic origin,

---

particularly HIV status); *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) (concerning cellular samples and DNA profiles); *Catt v United Kingdom* App no 43514/15 (ECtHR, 24 January 2019) (concerning data revealing political opinions).

[1058] C-136/17 *GC and Others,* Opinion of Advocate General Spzunar 10 January 2019 (ECLI:EU:C:2019:14), para 53.

[1059] C-136/17 *GC and Others* (ECLI:EU:C:2019:773), para 42.

[1060] ibid, para 43.

[1061] ibid, para 44.

[1062] ibid, para 67.

[1063] C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601) para 123-128.

[1064] Marvin Van Bekkum and Frederik Zuiderveen Borgesius, 'Using Sensitive Data to Prevent Discrimination by AI: Does the GDPR Need a New Exception?' (2022) 48 Computer Law & Security Review 105770, 14.

[1065] ibid 15.

[1066] Ludmila Georgieva and Christopher Kuner, 'Article 9. Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 369.

political opinions (and related trade union membership), religious or philosophical beliefs, and sexual life or orientation, data concerning health in particular.[1067]

Yet the manner in which such discrimination or harm is to be protected against under EU data protection law is relatively contained: specific to the use of sensitive personal data. Importantly, identifying features which might be the source of overt or targeted discrimination are only to be gathered in accordance with strict standards.[1068] The risk of discrimination and of impact upon fundamental rights is a risk which controllers are bound to have regard to in the implementation of their obligations.[1069] Automated decision making on the basis of sensitive personal data is further restricted.[1070] However, broader recognition of the risks of indirect discrimination, or the forces of oppression or domination which marginalised persons or communities can face which can heighten the effects of data misuse seems to be absent in the GDPR.

This might lead us to question whether the manner in which EU data protection law recognises such differences of identity are sufficient in order to ensure effective data protection of such persons and communities, or whether there are limitations in terms of harms associated with data protection which are capable of prevention or redress under EU data protection law. We can draw analogies to laws of anti-discrimination, which are often connected to data protection concerns in association with machine learning or automated/artificial decision making.

First we might ask – are the categories of identity or difference to be protected sufficient? In anti-discrimination law, Kirkland has written of protected characteristics as those differences which are recognised as legally significant.[1071] Hildebrandt has commented in a singular vein that "[p]eople are of course never entirely similar, so we need to know what difference *counts* and which difference should not be taken into account when governments decide on policies that affect their citizens and when they actually decide individual cases."[1072] We might therefore ask whether the differences which are recognised are sufficient in order to safeguard against discrimination in the context of data misuse.

One way of considering this is whether the categories might be considered under or over-inclusive. For instance, when we look to Article 21 of the EU Charter, discrimination on the basis of "any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."[1073] Immediately we can identify some inconsistencies, as Van Bekkum and Zuiderveen Borgesius have observed.[1074] Data which identifies sex is not considered sensitive personal data, for example, thus sex and gender-based discrimination is not expressly captured by the GDPR, despite ample historic discrimination on this basis.[1075] The curious position arises where

---

[1067] The addition of genetic and biometric data which identifies a given individual by the GDPR are similar if not quite the same.
[1068] As set out in Article 9(2), GDPR.
[1069] Recital 75, GDPR.
[1070] Article 22(4), GDPR.
[1071] Kirkland (n 997) 1.
[1072] Mireille Hildebrandt, 'Discrimination, Data-Driven AI Systems and Practical Reason' (2021) 7 European Data Protection Law Review 358.
[1073] Article 21, Charter.
[1074] Van Bekkum and Zuiderveen Borgesius (n 1064).
[1075] Implicitly, such discrimination might be challenged as "unfair" processing, though this is as yet untested.

trade union membership is protected as sensitive data, whereas other recognised protected characteristics are not.

Second, beyond questioning whether the particular categories of difference recognised in the sensitive personal data concept is sufficient, we might also question more broadly—is such a categorical approach of protecting difference sufficient to guard against data processing led discrimination? This may be questioned as a somewhat narrow understanding of discrimination; that which is expressly based on targeting of designated protected data. While many forms of algorithmic discrimination may be so captured,[1076] the possibility for discriminatory effect where the data enabling such discrimination is non-sensitive, seems to be excluded from the face of Article 9. For instance, Chen has warned that alongside the potential for direct and indirect discrimination, the "less noticeable but more disturbing" scenario of disparate impact, "where people are categorised and then treated differently with a multitude of factors taken into account in complicated, incomprehensible ways."[1077] Because of modern data inference possibilities, he argues that dangerous consequences for individuals or groups can arise "from some random, minor and untraceable initial differences."[1078] In other words, some discriminatory effects are not always attributable to direct or indirect discrimination. Wachter raises these concerns in the advertising context, pointing to the possibility of "affinity profiling," which does not rely on sensitive personal data, but some other shared affinity or group interest, which can be a marker/proxy for a protected characteristic.[1079] Barocas and Selbst have demonstrated a variety of ways in which further discriminatory this can occur.[1080] For example, protected characteristics need not be processed if new classes and labels are created through data inferences which are incidentally discriminatory, or where training data embeds bias in algorithms applied in a notionally neutral way, or where proxies or correlations for protected characteristics are used.[1081] These examples are illustrations of what Barocas and Selbst name institutional discrimination, and what is sometimes also named structural or systemic discrimination.

Much concern has been expressed about the potential of a gap in legal protection in relation to these inferential or incidental forms of discrimination. Wachter noted a legal grey area in 2020 when she wrote on the area,[1082] though the recent decision in *OT* suggests a broader capture of sensitive data on the basis of inference.[1083] The referring court had taken the view that information regarding sex life or sexual orientation could be deduced from the combination of the names of the declarants and their spouse, cohabitee or partner.[1084] The CJEU classified this inference as "an intellectual operation involving comparison or deduction",[1085] which certainly could be extended to other forms of inference. A purposive interpretation grounded the CJEU's determination that such indirect revelation of sensitive data must be deemed to fall within Article 9.

[1076] Jeremias Adams-Prassl, Reuben Binns and Aislinn Kelly-Lyth, 'Directly Discriminatory Algorithms' (2022) 86 The Modern Law Review 144.
[1077] Jiahong Chen, 'The Dangers of Accuracy' (2018) 4 European Data Protection Law Review 36, 41.
[1078] ibid 42.
[1079] Sandra Wachter, 'Affinity Profiling and Discrimination By Association in Online Behavioral Advertising' (2020) 35 Berkeley Technology Law Journal 367.
[1080] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
[1081] ibid.
[1082] Wachter (n 1079) 385.
[1083] C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601).
[1084] ibid, para 119.
[1085] ibid, para 120.

Article 9's approach is certainly not all encompassing, the categories of special data are not so broad as those contained in anti-discrimination law. Nevertheless, the CJEU's broad interpretation of the circumstances in which Article 9 is engaged, including for potential inferential uses of sensitive personal data does suggest a broader reach than perhaps some earlier literature expected.

4.2. Differences of decisional capacity: children and vulnerable data subjects

The second way in which we see EU data protection law expressly recognise difference between data subjects is through the addition of specific rules regarding the processing of the personal data of children and vulnerable data subjects.

The need to protect children specifically was a source of comment regarding the precursor regime under the Data Protection Directive.[1086] This criticism was met with a new specific set of protections which attach to children's data under the GDPR. The Recitals acknowledge the need for special protection, as children "may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[1087] This reflects an idea of the adult data subject as an agent in their own data protection, which is not deemed as realistic in the case of a child. Lievens and Verdoodt contrast this framing with the notion of informed decision making within the GDPR, writing it is "obvious that this process is more complex in relation to children."[1088] Malgieri and Niklas frame this as an issue of "decisional vulnerability.[1089] This echoes the notion of the empowered data subject discussed elsewhere.[1090] By contrast, the ECtHR has also recognised a heightened need to protect the privacy of children, but in a broader sense, in the name of "protecting his or her identity, well-being and dignity, personality development, psychological integrity and relations with other human beings, in particular between family members."[1091]

The additional protection which attaches to children under the GDPR takes a number of forms. First, we see how specific regard should be had for children when certain generalised data protection rules apply. With regards to the legal basis for processing, special regard must be had to a child's interest in the weighing of processing on the basis of legitimate interests.[1092] Intelligibility and accessibility of language is emphasised where information is provided to children.[1093] Data Protection Authorities are specifically tasked with raising public awareness in relation to processing of children's data.[1094] These specific considerations in

---

[1086] The Article 29 Working Party argued that the existing regime could be interpreted to satisfy children's needs in most cases, and other commentators expressed concerns. See ('General Guidelines and the special case of schools' (Article 29 Working Party 2009) 398/09/EN WP 160 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf>; Blume (n 59).

[1087] Recital 38, GDPR. The Recital then goes on to note areas where specific protection should apply, including marketing, profiling, and offering of services to a child.

[1088] Lievens and Verdoodt (n 244) 271.

[1089] Malgieri and Niklas (n 244) 6.

[1090] See Chapter 5.

[1091] *N.Š. v Croatia* App no 36908/13 (ECtHR, 10 September 2020), para 99.

[1092] Article 6(1)(f), GDPR provides: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[1093] Article 12(1), GDPR requires intelligible and accessible language "in particular for any information addressed specifically to a child."

[1094] Article 57(1)(b), GDPR requires DPAs "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention."

the application of general rules might be seen as mirroring the individualised differentiation of rules discussed in section 3 above.

In addition, special rules are in place for the processing of children's data in two key areas. A special regime is put in place with regard to children's consent to certain information society services.[1095] Such services, where offered directly to a child, are subject to an age of consent rule. A default age of 16 years is required in order for a child to be competent to consent (though national variation is permitted), and below this age parental authorisation is required. This limitation of a special consent rule to information society services is somewhat uneven.[1096] The result is to echo the notion of the data subject as a consumer, even as a child, and consent as type of transactional interaction, associated with services.[1097] In addition to this special regime for children's consent, a prohibition on automated decision making with legal or similarly significant effect regarding children is put in place.[1098]

The provisions on children's data protection represent the clearest recognition that some data subjects are in need of additional protection. The notion that some data subjects might be at risk of greater harm from data processing is briefly acknowledged in the Recitals to the GDPR, and in this recognition comes the link between children and vulnerable natural persons. Recital 75, which informs the risk-based approach which controllers are bound to consider in the implementation of their obligations, requires special consideration "where personal data of vulnerable natural persons, in particular of children, are processed".[1099] Malgieri and Niklas point to this Recital as the foundation for the idea that "some subjects should be protected not only because of their limited capacity to understand and give consent, but from higher risks of material or non-material damages."[1100] Yet if this is so, the protective effort is far from comprehensive, and might be said to reflect the lack of cohesive conceptualisation of paternalistic data protection strategies previously identified.[1101] This is an idea which receives no other attention in the GDPR in terms of substantive protections.

5. Reconciling difference: between individualisation and generalisation

EU data protection law has been characterised in the past as taking a uniform approach to its subjects.[1102] However, as I have demonstrated, some degree of difference is accommodated within its application through the individualisation of data subjects and through the recognition of some forms of difference between subjects.

Generalised provisions of the law which are framed in terms of the individual may require individual differentiation in order to be lawful. The Court has embraced specific individualised interpretations of such provisions in the area of transparency and subject rights, and we

---

[1095] Article 8, GDPR.
[1096] As Kosta notes, in the original draft of the GDPR, a general principle of consent was to require parental authorization of children's consent, but this was removed by time of final adoption. Eleni Kosta, 'Article 8. Conditions Applicable to Child's Consent in Relation to Information Society Services' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 356.
[1097] See also Chapter 3, Chapter 5.
[1098] Article 22, GDPR, read in light of Recital 71: "Such measure should not concern a child."
[1099] Recital 75, GDPR. See also 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (Article 29 Working Party 2017) 17/EN WP 248 rev.01 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en>. (Endorsed by the EDPB, 25 May 2018).
[1100] Malgieri and Niklas (n 244) 7.
[1101] See Chapter 5, GDPR.
[1102] Blume (n 59) 259.

might expect that such approaches would be followed in other areas of the GDPR which orient around individual protection.

Of course, the extent to which such differentiation of generalised rules is possible in practice may be linked to the enforcement and compliance challenges associated with individualised approaches at scale.[1103] Data controllers are likely better equipped to respond to individual circumstance and identity with specificity at smaller scale. Non-compliance becomes harder to detect and enforce by DPAs at great scale. Accordingly, in face of the reality of mass datafication and digitalisation, a vicious cycle emerges. The provisions are more likely to be violated or less equipped to deal with individual circumstances at scale, and the non-compliance is harder to police. One potential consequence which might result is an incentive to more data collection. In this sense, Van Bekkum and Zuiderveen Borgesius suggest more sensitive data collection may be necessary to prevent discrimination, and monitor anti-discrimination efforts.[1104] Individualised approaches may be contingent on controllers engaging in greater scrutiny of individuals in order to personalise responses to such individuals.

Some specific types of difference (certain identity signifiers and status as a child or vulnerable) attract special additional protection under the GDPR. Sensitive personal data, associated with some if not all protected characteristics, attracts heightened protection. The possibility to deduce sensitive personal data through inference has recently been confirmed as falling within this protection, an important extension of the protection in light of potential algorithmic forms of discrimination. Children's decision making in the context of certain online services is to be safeguarded by their parent, as doubt exists as to their capacity to engage in the decision making process regarding personal data choices.

However, no comprehensive regard to diversity or difference between data subjects is evident in EU data protection law. The reality that some data subjects will be better equipped or disposed to avail of the protections of the law, that some will face greater harm, and that some will be excluded from it is worth remembering. This resonates with historic critiques of privacy as a right of the privileged.[1105] As Boyle has cautioned, we should remember that by critiquing subjectivity, we can ask "Who gets to be a subject? What qualities or attributes about them are included in the box of subjectivity and what attributes are excluded?"[1106] And thus, certain assumptions about capacity and the circumstances of data subjects are apparent within the GDPR, and can operate to exclude or further marginalise those who do not meet these assumptions.

Such exclusionary assumptions could raise issues under the Charter, as those who are excluded from protection within the terms of the GDPR are being denied their fundamental rights. The link between deficient implementation or operation of the GDPR and fundamental rights has been suggested in the context of the national procedural nature of representational actions. González Fuster has pointed out that where actions "are not

---

[1103] See Chapter 3.

[1104] Van Bekkum and Zuiderveen Borgesius (n 1064).

[1105] Monahan and Murakami Wood look to the historical development of the right to privacy in the US and argue that "privacy was mobilized as a right of the privileged." They raise the concern over "unequal access to privacy rights, even during its emergence as a legal construct over a century ago," as a possible explanation for the concerns which surveillance scholars have about privacy discourses. Torin Monahan and David Murakami Wood, 'Surveillance Studies as a Transdisciplinary Endeavor' in Torin Monahan and David Murakami Wood (eds), *Surveillance Studies: A Reader* (Oxford University Press 2018) xxiii.

[1106] In Boyle's study on the legal subject, he points to the value of critiquing subjectivity, just as objectivity has been scrutinised by critical legal theorists. Boyle (n 17) 511.

equally available to all data subjects," there is a potential clash with "the fundamental rights nature of EU data protection, the need to provide effective remedies of EU law, and the EU's commitment to the promotion of the right of consumers to organise themselves in order to safeguard their interests."[1107] We can extend this, through the suggestion by the Advocate General in *TU, RE v Google* that a requirement to bring national procedural actions to make a right to be forgotten request to a search engine might be a disproportionate sacrifice of Charter rights (citing Article 7 and 8).[1108] If we are to read the GDPR in light of these Charter rights, together with the right to an effective remedy under Article 47 of the Charter, it becomes apparent that the rights of all are not being equally met by the GDPR. In this way, an inadequate consideration of the diversity of data subjects comes to undermine the GDPR's capacity to achieve its aims.

The tension between individualisation and generalisation identified in this chapter is perhaps representative of the broader trade offs within EU data protection law, and tensions between different legal approaches to fundamental rights. An individual approach, rooted in a liberal idea of individual uniqueness, allows for treatment of the person *as individual,* to take account of their particular identity and circumstances. Thus, differentiation is possible, and in the hands of DPAs and courts, or when asserted by a capable subject, particularisation is possible. When there is no one universal vision of the desirable level of data protection, an individual case-by-case approach may be the best approach to try to satisfy a majority. Nevertheless, the abstracted notion of the individual as contained in the law may represent assumptions of capacity and circumstance which has the effect of excluding some persons from participation within the regime, and aside from a single reference to "vulnerable data subjects", such persons are not addressed in the regime. On the other hand, individualised approaches can be challenging to apply at scale. Individuals, DPAs and courts are all less able to supervise interferences with data protection interests on an individualised basis in an era of datafication and informational capitalism. When data exists in relational and plural forms, conflicts of individual preference or impact may arise. This puts more pressure on collective enforcement mechanisms and developing paternalistic approaches to data protection, to protect individuals when their own decision making or action is either inappropriate or impossible. In the conclusion, I will offer some thoughts on what this uncomfortable tension and variety of trade-offs tells us about the place and idea of the individual in EU data protection law.

[1107] Gloria González Fuster, 'Article 80. Representation of Data Subjects' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 1150.
[1108] C-460/20 *TU, RE v Google* Opinion of Advocate General Pitruzzella, 7 April 2022 (ECLI:EU:C:2022:271) paras 38-40.

CONCLUSION

This thesis has offered an account and evaluation of the role and conception of the individual within EU data protection law. I have argued that the individual's role is central to EU data protection, though we should not characterise the regime as entirely individualistic. The individual is at the centre of the normative underpinnings of EU data protection, though without particularly detailed understandings of the substance of what data protection is trying to achieve, especially in default of individual control of data. The legal architecture which seeks to protect that individual right is made up of different layers, with individualised, collective, procedural and structural approaches in evidence. At these different levels, the individual's multi-faceted role engages different normative and practical concerns.

Moreover, the *idea* of the individual has shaped EU data protection law, which can be connected in part to the historical and institutional context in which EU data protection law developed. This idea, or rather multiple ideas of the individual, once explored, reveal certain assumptions and theories manifest in the legal regime. Often fragmentary visions emerge, and key tensions in EU data protection law may be associated with the question of these notions of the individual – including the clash between rights-based and economic visions of the subject, the capacity of individualised approaches to deal with interdependence and interconnection, the balance between empowerment and paternalistic protection or restriction of the subject and the capacity of the law to protect differently positioned subjects. Re-engaging with ideas of the person which underpin EU data protection law is necessary in order to come to grips with these tensions—in other words, the conceptual role of the individual can guide the practical implementation of their protection through EU data protection law.

In this concluding chapter, I summarise the findings of this thesis, situate these findings in terms of the thesis's contribution, and offer some thoughts on where these ideas might be developed further in future research.

1. The role and conception of the individual in EU data protection law

The individual, both as idea and actor, are central to the EU data protection project.

This centrality derives from multiple aspects of the regime. The notion of their right to and interest in data protection form the normative basis which grounds the legislative project of the GDPR, though the content of this right and interest can be vaguely expressed and difficult to disentangle from notions of individual privacy. The individual's status as legal subject within the regime holds many forms: a rightsholder under the Charter, at times a data subject or a data controller, or another affected natural person. The individual is also an important agent of data protection law, in their role in the private enforcement of EU data protection law, and as a decision-maker who performs the idea of control of data. Seen in this multi-faceted way, each element of the individual's role may be questioned, to look beyond a general question of the extent of *individualism* in EU data protection law*,* and ask more nuanced question about the role the individual is playing, the relationship between aspects of this role and the interaction between the individually oriented aspects of the legal regime and the remainder of the regime.

In identifying the individual as the normative foundation of EU data protection law, I am not advocating for this position of the individual, but rather I have sought to engage with the consequences of this normative function from a legal perspective. The central normative position of the individual means that group or societal concerns or interests in data

protection have largely not been integrated into the legal regime. Accordingly, the conception of the importance of data protection takes on a particularly individualistic sense in the case law of the CJEU, and there does not seem to be an acknowledgement of any collective or communal interest in data protection.

Ultimately, I have not taken a position on whether the individual should be an object or normative basis of EU data protection law. I believe this question is fundamentally a contested question of political philosophy (i.e. whether a liberal political order is desirable, or whether the individual is the best unit of social good), which engages philosophical and political theories which are beyond the boundaries of my thesis, which is a legal endeavour. Rather, I have sought to make analytical contributions on the manner in which this normative objective has been implemented, i.e. the consequences and limitations of the current model in terms of legal effect. In doing so, I have re-surfaced the question of the individual as an object for discussion, which I hope might inform a broader normative debate on the matter in the future.

The question of whether the individual should be placed as a central legal subject, in a variety of guises, and as an agent in the performance of EU data protection law, I understand as connected to concerns of legal/regulatory design and effect, and are analysed and more deeply engaged with in the remainder of my thesis.

Specifying and examining the role of the individual as a legal subject (as a rights-holder, the data subject, and other protected natural persons) allows us to consider some of the consequences of a primarily individualised understanding of the data subject. This individually-oriented conception of the subject, linked to the material scope of EU data protection law, may be said to be challenged in an environment of mass datafication, as individualised approaches have a scaling effect which can undermine individual and public oversight of data processing. Challenges of breadth can be contrasted with a more targeted approach seen in the notion of sensitive personal data, and offer a point of comparison in terms of the necessary individuality of the subject. The phenomenon of the individual being captured as a regulated subject, as a data controller, may be seen as a reflection of this same expansionist tendency, as the CJEU has broadened the interpretation of the controller, while narrowing the purely personal and household processing exemption. As a result, the notional desire to protect individuals has increased the likelihood that some individuals will be captured as regulated subjects. This results in a mismatch between legal allocation of responsibility and practical capacity to meet that responsibility given the bureaucratic nature of many of the obligations attached to controllers.

The role of the individual as an agent in the operation of data protection law, through the exercise of informational decision making and the exercise of data subject and procedural rights calls into question whether the individual is being empowered or improperly responsibilised in an environment in which self-defence is very challenging due to mass datafication. This raises concerns that the formal availability of means of self-defence which cannot or are not being practically exercised can lead to the sheltering of abusive practices from legal scrutiny, and re-engages questions of the social or public responsibility to ensure the operation of data protection law.

All of these questions as to the consequences of the role that the individual plays necessarily paint a one-sided picture. Those aspects of EU data protection law which are not individually oriented are introduced, and we remember that other normative interests are incorporated into the regime, even if to a lesser legal effect than individual data protection. Other subjects have important roles to play, particularly the controller, whose nature and activities do shape

the measurement of their legal obligations but which has not had the same impact upon the framing or scope of the law.

Bringing the non-individualist counter-parts into the discussion opens up the question of the extent of the individualism of the regime, and allows us to both see the centrality of the individual in terms of their impact on key aspects of the regime and also the limits to their legal function and role. Moreover, we recognise that this individualism is not absolute, in the sense that the individual interest is not the only relevant consideration, nor that the individual is the only subject with status or power in the legal regime. For these reasons, I characterise the individual as central to the regime, but do not consider it entirely individualistic. Additionally, in questioning the balance between the individualist and non-individualist aspects of the law, we can think holistically about the choices (express and implicit) which characterise the regime, and also re-engage with the possibilities of structural protection which are contained within the law.

In order to move forward, and problematise the individual's role and conception in greater depth, I look to how ideas of the individual have shaped EU data protection law, and why the individual has taken on such prominence in this field. I argue that the reasons for the centrality of the individual to the regime can be associated with two contextual sources: the historical and conceptual connection to rights of privacy and respect for private life, which is primarily understood as relating to the individual and an order of fundamental rights, and the EU political and institutional context. By reminding ourselves of these connections, we can contextualise in part the prevailing conceptions of the individual within the regime—the notion of individual control over data, and the balance between the individual as economic actor and their status as a rights-holder. This reveals an understanding of the individual's role as one that has been contextually influenced. The early liberal rights orders still have resonance with the position and conception of the individual in EU data protection law, but we see that the concerns of power which were central to early liberal theorists of privacy have become less prominent, and rather competing interests come into a rights "balancing" framework. The EU supranational context has also shaped the position of the individual in data protection law, as the individual and their fundamental rights are central to the EU legal order, and the EU's vision of a socio-economic order is premised upon individual economic freedom and action.

This contextualisation also invites us to open up the question of conceptions or ideas of personhood, and how these can manifest in certain functions or understandings of the individual in data protection law. The sometimes tension between an economic or marketized understanding of the data subject is contrasted with a rights-oriented vision of the citizen subject, as rights balancing features more strongly with respect to public sector data processing, while private sector processing tends to be treated in more transactional and marketized terms.

A more contextualised understanding of the individual's position in EU data protection law offers a number of insights. First, we can remind ourselves that ideas of privacy, private life, and of individual rights have been varied and diverse since their early development, and thus remember that current manifestations of these ideas are not immutable. Second, by noting that multiple conceptions of individuality and personhood have been in co-existence for as long as we have been developing and debating ideas of privacy, we can also recognise that alternative conceptions are possible, find foundations and historical precedents for non-individualist conceptions of data protection, and question what it is about the current moment or context that has led to the elevation or increased prominence of individualist aspects, or particular conceptions of personhood.

The study of the place of the individual continues through the question of how ideas of personhood may be identified from the legal treatment of the individual. I offer three case studies of approaches to personhood, and how they relate to the conception of the person in data protection law. Each reflects a dimension of personhood: individuation versus interdependence, empowered versus the subject of paternalistic protection and homogenous versus diverse.

In considering the phenomenon of data sets which capture multiple persons' data, through the concept of *plural personal data* the vision of the individual which appears from the regime is primarily individuated. Plural personal data can exist as inherently plural data, where it captures or records an existing relationality between the data subjects (such as social, biological or environmental tie), or as developed plural data, where data has been amalgamated into a large dataset which relates to more than one person, for the purpose of surveillance or analytics. Datafication, the co-option of social spaces by informational capitalism and the growth of "big data" analytics have intensified the creation and exploitation of plural personal data. Plural personal data are considered in the light of some central aspects of EU data protection law, which reveals a tension between the existence of plural personal data and the individualist aspects of EU data protection law. While there is some recognition of the existence of relational data, this is fragmented and does not betray any consistent regard for the phenomenon of inherently plural personal data or developed plural personal data.

Importantly, even though there might be some minimal regard for the fact that plural personal data may be captured simultaneously, this recognition has not let to legislative consideration or judicial acknowledgment of how individually oriented aspects of the law might need adaptation in their application to plural personal data. The data subject rights suggest a language of balancing, but the nature of such balancing is not explored, and may be challenging to implement the more data subjects are involved. In assessing the legality of processing, the application of individualised standards to plural personal data raises possibilities of conflict or unequal treatment between differently placed data subjects. Generalised standards, such as the data protection principles, may be more adaptable to plural personal data, but concerns as to differential impact persist. At an enforcement stage, the same issues arise–the potential for misalignment between the interests or harms felt between individuals in the same plural personal dataset mean that individually exercisable rights may lead to clashes of position. The aggregative nature of the collective envisaged by representative actions may be a useful tool to respond to plural personal data abuses (if a collective enforcement practice substantially materialises), but again, are more suitable when interests are aligned. All of this highlights the absence of consideration of the ways in which data subjects exist in relation and interdependently with others, which challenges those aspects of the law which are founded on either individualist legal approaches, and more generally, highlights the absence of regard for how generalised provisions may apply at scale, to a diverse pluralistic population. The conception which emerges is primarily that of an individuated, standalone individual data subject.

EU data protection law balances strategies of individual empowerment and paternalistic strategies (i.e. legal approaches which restrict or substitute individual choice). At a substantive level, the individual's choices over data usage are relatively narrow—based on a strict conception of consent, and contractual choice, though an individual's refusal of processing is not necessarily fatal as the controller may be able to satisfy other legal bases. A protective paternalism is more prominent, as the individual interest is still foremost, but the decision making over data lays elsewhere. At a procedural level, the rights to access, portability and objection provide the data subject with some participation in the treatment of

their data, while the remainder of the rights might be more properly classified as tools of self-defence. A picture primarily of individual responsibilisation rather than empowerment emerges. At a structural level, the law places some emphasis on requiring controllers and national regulators to protect individual choice, as they are required to take into account the risk of loss of control of data when implementing controller obligations and legislative derogations to protections. On the other hand, the notion that the controller is the primary decision making entity over data may be said to cement an idea of bureaucratically and organisationally driven data processing, and thus a vision of the law responding to a status quo rather than trying to re-invent or support new means or structures of individual empowerment.

The picture which results is less concerned with individual empowerment than with a sense of individual protection in the hands of the controller, legislator, DPAs and courts. Yet the strategy or foundations of the paternalistic approach are not evident, and in contrast to the rather prominent ideas of informational self-determination, a theory of protective paternalism does not cohere. This may go some way to explain the vague operation and sometimes questionable consequences of the CJEU's device of "complete and effective protection" in its judgments. There is a lack of normative foundation for the operationalisation of paternalistic protection. To the extent that individual empowerment does exist in the law, the vision of the data subject which emerges is a marketized actor. Ideas of data as an economic asset and the subject as a type of consumer or economic participant are reflected in the ways in which consent and contractual relations under EU data protection operate.

In questioning how EU data protection law understands and responds to difference between subjects, an illustration of the balance between individualisation and generalisation in the law emerges. Individually tailored legal standards and individually exercisable rights are oriented to particular circumstances, and the CJEU has confirmed that many of these provisions must respond to a given individual's own case. This demonstrates a degree of flexibility and capacity to accommodate difference between affected individuals. Nevertheless, assumptions regarding capacity, circumstance and resources may still exclude some individuals from participating in these processes or the exercise of their rights. Some forms of difference are expressly recognised and acted upon; differential impact of data harms are recognised through the protection of sensitive personal data, though these may not address all forms of data driven discrimination. Differences of decisional capacity are also recognised through the addition of a special regime of children's consent, though only with regard to certain online services, and in the requirement that controllers are bound to have regard to risks to children and vulnerable data subjects. No comprehensive regard or theory of difference seems to emerge, but rather a pragmatic response to some known harms, and questions remain as to whether some persons or harms are underserved or excluded by EU data protection law.

These tensions which emerge—between the individual and the collective, between relationality and individuation, between empowerment and paternalism, between difference and uniformity all go to the heart of key dilemmas of EU data protection law. The place and understanding of the individual highlight *inter alia* the challenges of (1) contending with scale and structural forces such as big data, datafication or informational capitalism, (2) enforcing data protection law, and (3) the capacity of the law to meaningfully redress individual and other harms of a pluralistic and interdependent populace. More fundamentally, by revealing these tensions, curious silences in the law are noticed. How is the individual to be served by data protection? What is the desirable balance between competing concerns? We are once again left with questions as to the conceptual foundations of data protection, and how its

normative mission to protect individuals is to be realised. The fragmentary picture of the individual thus mirrors a fractured foundation.

Given the centrality of the individual to so many aspects of EU data protection law, the lack of coherent or comprehensive normative grounding of the nature of the individual interest, and how that connects to the design and operation of EU data protection law has disadvantages. Along with a number of scholars who have pointed to the need for more robust conceptualisation of the aims of data protection law,[1109] I suggest that the lack of clarity or specificity of the understanding of the individual and their protection in particular is having knock-on consequences, some of which is limiting the capacity of the law to achieve its self-described mission.

By understanding and questioning a central plank of the regime, new questions and critiques emerge. In recognising the fragmentary and incomplete ideas of personhood which permeate data protection law, I have introduced new considerations to the debate on the effectiveness of EU data protection law. The consequence is that my contribution on the question of whether individualist approaches to privacy and data protection are desirable has been both to refine and complicate. A refinement, in offering more nuanced questions on how we might explore this issue, and reframing the choices and assumptions which have underpinned aspects of the individual's legal role within EU data protection law. A complication, in recognising that there are no easy answers to these questions, that there are tensions and conflicts between choices made, and unfortunately any outcome in terms of legal settlement between interests is likely to have trade-offs and disadvantage some parties.

2. The significance of these conclusions

First, I have provided a detailed conceptual framework of the individual in EU data protection law. This offers not a normative model of the individual, but an understanding of the ways in which the individual is relevant to EU data protection law. In understanding the multi-faceted role of the individual, and the importance of the individual to key aspects of EU data protection law I have illustrated the centrality of the individual to the regime, as well as offered an analytical framework against which we can question these facets both separately and in totality. Once we come to question these various facets, limitations of those individualist aspects are surfaced, but at the same time in recognising the limits to the individual's role, and other actors and interests which are also represented in EU data protection law I have also provided a rejoinder to those who would classify the regime as an entirely individualist one.

Second, I have demonstrated the relevance of complex and conflicting ideas of personhood to the question of the individual in EU data protection law. The place of the individual, or individualist strategies in EU data protection law has been of increased attention in recent years, though structural and social views of privacy have a long history. I suggest this debate is enriched by engaging with the theories (including philosophical or ideological) which underpin the role of the individual. In this sense, my thesis has illustrated the value of looking both within and without—within the law to see how the individual is understood, and the assumptions or ideas which have so become embedded, and without, to the context in which the law evolved, to question where such assumptions or ideas have originated. In doing so, I have argued that there are implicit features to the place of the individual, and by re-surfacing

[1109] Including Bygrave, 'The Body as Data?' (n 715); Purtova, 'From Knowing by Name to Targeting' (n 86); Lynskey, 'Delivering Data Protection' (n 249).

some of these assumptions or values from the implicit to the explicit new understandings and analysis of EU data protection law are possible.

3. Future questions

This thesis was ambitious in its scope, but I hope it represents not the end of a journey but a beginning. Three categories of issues may be said to be suggested by the work to date but which will necessitate more work to further explore.

First, the thesis has investigated the link between a fundamental right and the legislative scheme which seeks to protect that right. While the right to data protection has some unique factors, there is a broader debate in human rights theory about the capacity of liberal rights frameworks to deal with *inter alia* structural and material issues, or achieve justice more generally.[1110] By connecting the right to data protection to this broader literature on liberal rights and individualism, connections may be drawn to other fundamental rights, particularly those which are conceived in terms of positive obligations by States, and to other literatures on rights theory. This connects to the broader issue of liberalism in EU data protection law, and whether an individual rights-based approach is the appropriate normative vision for the law.

Second, this thesis has not sought to conceptualise collective or group models of data protection. Nevertheless, the questions of assumptions of personhood embedded in our idea of the individual have illustrated the question of regulatory or legal approaches cannot be flattened into a individual vs. collective binary. Rather, I have argued that to assume that a collective approach will redress perceived failings of individualist approaches is to see only part of the picture, and to make great assumptions about the nature of individuals (and presumably about the nature of collectives.) Accordingly, a valuable complement to or extension of this work could be the exploration of how diverse ideas of collectivity (e.g. the public, the communal, pluralities) can offer alternatives or additions to individualised approaches.

Third, if as it seems, that EU data protection has become more concerned with the individual over time,[1111] over other governance approaches, we can question why current policy agendas or modes of regulatory approach have been elevated, and a liberal (or neoliberal) individualism has the particular role it has in EU data protection law. By re-engaging with the EU institutional and political context of which data protection is part, future research might connect these patterns in legislative and regulatory approach with broader patterns of EU constitutional change and political economy.[1112]

Thus, the work has only begun.

[1110] This is a large field of study, but by way of example, see Douzinas (n 12); Costas Douzinas, 'The Paradoxes of Human Rights' (2013) 20 Constellations 51; Susan Marks, 'Four Human Rights Myths' in David Kinley, Wojciech Sadurski and Kevin Walton (eds), *Human rights: Old Problems, New Possibilities* (Edward Elgar Publishing Ltd 2013); David Kennedy, 'The International Human Rights Movement: Part of the Problem?' in Robert McCorquodale (ed), Robert McCorquodale, *Human Rights* (1st edn, Routledge 2017).

[1111] As Van der Sloot argues and Mayer-Schönberger has observed. van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They?' (n 60); Mayer-Schönberger (n 911).

[1112] For example, see Alexander Somek, 'European Constitutionalism: The Neoliberal Drift' (*LPE Project*, 11 April 2019) <https://lpeproject.org/blog/european-constitutionalism-the-neoliberal-drift/> accessed 20 February 2023; Bojan Bugaric, 'The Neo-Liberal Bias of the EU Constitutional Order: A Critical Analysis' in Mark Tushnet and Dimitry Kochenov, *Research Handbook on the Politics of Constitutional Law* (Edward Elgar Forthcoming) <https://www.ssrn.com/abstract=4353114> accessed 20 February 2023.

BIBLIOGRAPHY

1. TREATIES, CONSTITUTIONS, LEGISLATION AND OTHER INSTITUTIONAL SOURCES

1.1. Treaties and international law

Universal Declaration of Human Rights

International Covenant on Civil and Political Rights

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

The Treaty on European Union

The Treaty on the Functioning of the European Union

Charter of Fundamental Rights of the European Union

1.2. National constitutions

Austrian Constitution of 1867. https://ecommons.cornell.edu/server/api/core/bitstreams/72052edc-e746-4adf-a397-3197154233a2/content

Federal Constitutional Act of Austria. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.html

Belgium's Constitution of 1831 https://www.constituteproject.org/constitution/Belgium_1831

The Belgian Constitution (English translation) https://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/GrondwetUK.pdf

Constitution of Bulgaria, 1879. Translation available in Herbert F. Wright (ed) *The constitutions of the states at war,* 1914-1918. (US Govt, 1919) https://archive.org/details/constitutionsofs00wrig/page/n5/mode/2up

Constitution of Bulgaria, Article 32. https://www.parliament.bg/en/const

Constitution of the Republic of Croatia (consolidated text). https://www.sabor.hr/en/constitution-republic-croatia-consolidated-text

The Constitutional Act of Denmark, s72. https://www.thedanishparliament.dk/-/media/sites/ft/pdf/publikationer/engelske-publikationer-pdf/the_constitutional_act_of_denmark_2018_uk_web.pdf

Charter of Fundamental Rights and Freedoms of the Czech Republic, https://www.psp.cz/en/docs/laws/listina.html

The Constitution of the Republic of Estonia. https://www.riigiteataja.ee/en/eli/521052015001/consolide

The Constitution of Finland https://finlex.fi/en/laki/kaannokset/1999/en19990731_20180817.pdf

Constitution of France, 1958 https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/anglais/constiution_anglais_oct2009.pdf

Basic Law for the Federal Republic of Germany, https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html

Constitution of Greece https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156 aggliko.pdf

The Fundamental Law of Hungary, https://2015-2019.kormany.hu/download/a/68/11000/The_Fundamental_Law_of_Hungary_01072016.pdf

Constitution of Ireland / Bunreacht na hÉireann 1937 https://www.irishstatutebook.ie/eli/cons/en/html

Constitution of the Italian Republic 1947 https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf

The Constitution of the Republic of Latvia, https://www.saeima.lv/en/legislative-process/constitution

Constitution of Lithuania, https://www.constituteproject.org/constitution/Lithuania_2006

Constitution of Luxembourg https://www.constituteproject.org/constitution/Luxembourg_2009

Constitution of Malta, https://legislation.mt/eli/const/eng

Constitution of the Kingdom of the Netherlands https://www.government.nl/documents/reports/2019/02/28/the-constitution-of-the-kingdom-of-the-netherlands

Constitution of the Republic of Poland https://constituteproject.org/constitution/Poland_2009

Constitution of the Portuguese Republic https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf

Constitution of Romania https://www.presidency.ro/en/the-constitution-of-romania

Constitution of the Republic of Slovenia https://www.us-rs.si/media/constitution.pdf

The Spanish Constitution https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf

Instrument of Government of Sweden. the Spanish Constitution https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf

1.3. EU Secondary Legislation

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995, p 31–50).

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/7/2002, p 37–47) 200.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4/5/2016, p 1–88).

DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4/5/2016, p 89-131).

COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (OJ 2016 L 207, p. 1.)

COMMISSION DECISION OF 5 FEBRUARY 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by COMMISSION IMPLEMENTING DECISION (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21/11/2018, p.39-98).

DIRECTIVE (EU) 2020/1828 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409/1, 4/12/2029, p 1–27).

REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12102022, p 1–66);

REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277/1, 27102022, p 1-102).

1.4. Regulatory Guidance

‘Opinion 4/2007 on the Concept of Personal Data’ (Article 29 Working Party 2007) 01248/07/EN WP 136 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>

‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (Article 29 Working Party 2014) 844/14/EN <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>

‘General Guidelines and the special case of schools’ (Article 29 Working Party 2009) 398/09/EN WP 160 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf>

‘Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679’ (Article 29 Working Party 2017) WP251. <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision making-and-profiling_en>

‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’ (Article 29 Working Party 2017) 17/EN WP 248 rev.01 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en>

Guidelines on the Right to Data Portability’ (Article 29 Working Party 2017) 16/EN WP 242 rev.01 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>

‘First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities’ (European Data Protection Board 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> accessed 28 April 2019

‘Guidelines 05/2020 on Consent under Regulation 2016/679’ (European Data Protection Board 2020) Version 1.1. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>

1.5. Other EU institutional sources

‘Community Policy on Data Processing’ (Commission of the European Communications 1973) Communication of the Commission to the Council SEC(73) 4300 final <http://aei.pitt.edu/6337/1/6337.pdf> accessed 8 February 2021

‘Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing’ (European Parliament 1979) OJ C 140/34 <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1979%20-%20European%20Parliament%20Resolution%20on%20DP.pdf> accessed 12 February 2021

Commission Communication on the protection of individuals in relation to the processing personal data in the Community and information security. COM(90) 314 final – SYN 287 and 288. 13 September 1990.

‘Data Protection in the European Union: The Role of National Data Protection Authorities’ (European Union Agency for Fundamental Rights 2010) https://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM/2010/0609 final. 4 November 2010.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD).

1.6. Other

'Human Rights and Modern Scientific and Technological Developments' (Council of Europe 1968) Assembly Debate on 31st January 1968 (16th Sitting) Recommendation 509 <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en> accessed 8 February 2021

'Records, Computers and the Rights of Citizens' (US Department of Health and Human Services 1973) <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> accessed 16 February 2021

Resolution (73) 22 <https://rm.coe.int/1680502830> accessed 3 December 2023

'Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector' (Committee of Ministers of the Council of Europe 1974) Resolution (74) 29 <https://resources.law.cam.ac.uk/cipil/travaux/1974%20-%20Resolution%2074(29)%20on%20Privacy%20EDB%20&%20Public%20Sector.pdf> accessed 12 February 2021

'How to Disclose Information Safely: Removing Personal Data from Information Requests and Datasets' (Information Commissioner's Office 2018) <https://ico.org.uk/media/2013958/how-to-disclose-information-safely.pdf>

'Guide on Article 8 of the European Convention on Human Rights' (Council of Europe 2020) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> accessed 8 February 2021

2. CASES

2.1. Cases of the CJEU

Case 215/88 *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung* (ECLI:EU:C:1989:331)

C-369/98 *Fisher* [2000] ECR I-6773

Joined cases C-122/99 P and C-125/99 P *D and Sweden v Council* (ECLI:EU:C:2001:304).

C-450/00 *Commission v Luxembourg* [2000] ECR I-7074

Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* [2003] ECR I-5014

C-101/01 *Lindqvist* [2003] ECR I-12992

Joined cases C-317/04 and C-318/04 *Parliament v Council (PNR)* [2006] ECR I-04721

C-275/06 *Promusicae v Telefónica de España* [2008] ECR I-00271

C-524/06 *Huber v Germany* [2008] ECR-I-09705

C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-09831

C-518/07 *Commission v Germany* [2010] ECR I-01885

C-553/07 *Rijkeboer* [2009] ECR I-03889

C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* [2009] ECR I-01227

C-28/08 P *Commission v Bavarian Lager* [2010] ECR I-06055

C-92/09 *Volker und Markus Schecke and Eifert* [2010] I-11063

C-543/09 *Deutsche Telekom* [2011] I-03441

C-70/10 *Scarlet Extended* [2011] I-11959

C-360/10 *SABAM* (ECLI:EU:C:2012:85)

C-461/10 *Bonnier Audio and Others* (ECLI:EU:C:2012:219)

C-614/10 *Commission v Austria* (ECLI:EU:2012:631)

Joined cases C-468/10 and C-469/10 *ASNEF* [2011] I-12181

C-131/12 *Google Spain and Google* (ECLI:EU:2014:317)

Joined cases C-141/12 and C-372/12 *YS and Others* (ECLI:EU:C:2014:2081)

C-288/12 *Commission v Hungary* (ECLI:EU:C:2014:237)

C-291/12 *Schwartz* (ECLI:EU:C:2013:670)

Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (ECLI:EU:C:2014:238)

C-342/12 *Worten* (ECLI:EU:C:2013:355)

Joined cases C-446/12 to C-449/12 *Willems and Others* (ECLI:EU:C:2015:238)

C-473/12 *IPI* (ECLI:EU:C:2013:715)

C-486/12 *X* (ECLI:EU:C:2013:836)

C-212/13 *Ryneš* (ECLI:EU:2014:2428)

C-580/13 *Coty Germany* (ECLI:EU:C:2015:485)

C-201/14 *Bara and Others* (ECLI:EU:C:2015:638)

C-230/14 *Weltimmo* (ECLI:EU:C:2015:639)

C-235/14 *Safe Interenvios* (ECLI:EU:C:2016:154)

C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650)

C-582/14 *Breyer* (ECLI:EU:C:2016:779)

Opinion 1/15 *Passenger Name Record Agreement* (ECLI:EU:C:2016:656)

C-191/15 *Verein für Konsumenteninformation* (ECLI:EU:C:2016:612)

Joined cases C-203/15 and C-698/15 *Tele2 Sverige* (ECLI:EU:C:2016:970)

C-398/15 *Manni* (ECLI:EU:C:2017:197)

C-13/16 *Rīgas satiksme* (ECLI:EU:C:2017:336)

C-73/16 *Puškár* (ECLI:EU:C:2017:725)

C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388)

C-311/18 *Facebook Ireland & Schrems* (ECLI:EU:C:2020:559).

C-434/16 *Nowak* (ECLI:EU:C:2017:994)

C-498/16 *Schrems v Facebook Ireland Ltd* (ECLI:EU:C:2018:37)

T-670/16 *Digital Rights Ireland v European Commission* (ECLI:EU:T:2017:838)

C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551)

C-40/17 *Fashion ID* (ECLI:EU:C:2019:629)

C-136/17 *GC and Others* (ECLI:EU:C:2019:773)

C-345/17 *Buivids* (ECLI:EU:C:2019:122)

C-496/17 *Deutsche Post* (ECLI:EU:C:2019:26)

C-507/17 *Google France v CNIL* (ECLI:EU:C:2019:772)

C-623/17 *Privacy International* (ECLI:EU:C:2020:790)

C-673/17 *Planet49* (ECLI:EU:C:2019:801)

C-311/18 *Data Protection Commissioner v Facebook Ireland* (ECLI:EU:C:2020:559)

C-511/18 *La Quadrature du Net and Others* (ECLI:EU:C:2020:791)

C-61/19 *Orange Romania* (ECLI:EU:C:2020:901)

C-645/19 *Facebook Ireland and Others* (ECLI:EU:C:2021:483)

C-817/19 *Ligue des droits humains* (ECLI:EU:C:2022:491)

Joined cases C-37/20 and C-601/20 *WM, Sovim SA v Luxembourg Business Registers* (ECLI:EU:C:2022:912)

C-140/20, *Commissioner of an Garda Síochána and Others* (ECLI:EU:C:2022:258)

C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (ECLI:EU:C:2022:601)

C-319/20 *Meta Platforms Ireland* (ECLI:EU:C:2022:322)

C-460/20 *TU, RE v Google* (ECLI:EU:C:2022:962)

C-534/20 *Leistritz* (ECLI:EU:C:2022:495)

C-77/21 *Digi* (ECLI:EU:C:2022:805)

C-132/21 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECLI:EU:C:2023:2)

C-154/21 *RW v Österreichische Post AG* (ECLI:EU:C:2023:3)

C-300/21 *Österreichische Post AG* Opinion of Advocate General Campos Sánchez-Bordona 6 October 2022 (ECLI:EU:C:2022:756)

2.2. Cases of the European Court of Human Rights

Z v Finland App no 22009/93 (ECtHR, 25 February 1997)

Amann v Switzerland App no 27798/95 (ECtHR, 16 February 2000)

PG and JH v United Kingdom App no 44787/98 (ECtHR, 25 September 2001)

Pretty v. United Kingdom App no 2346/02 (ECtHR, 29 April 2002)

Peck v United Kingdom App no 44647/98 (ECtHR, 28 January 2003)

Odievre v France App no 42326/98 (ECtHR, 13 February 2003)

Perry v United Kingdom App no 63737/00 (ECtHR, 17 July 2003)

S and Marper v United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008)

Reklos and Davourlis v Greece App no 1234/05 (ECtHR, 15 January 2009)

Von Hannover v Germany (No. 2) Apps nos 40660/08 and 60641/08 (ECtHR, 7 February 2012)

Radu v Moldova App no 50073/07 (ECtHR, 15 March 2014)

MN and Others v San Marino App no 28005/12 (ECtHR, 7 July 2015)

Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016)

A-MV v Finland App no 53251/13 (ECtHR, 23 March 2017)

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland App no 931/13 (ECtHR, 27 June 2017).

Bărbulescu v Romania App no 61496/08 (ECtHR, 5 September 2017)

Antović and Mirković v Montenegro App no 70838/13 (ECtHR, 28 November 2017)

Benedik v Slovenia App no 62357/14 (ECtHR, 24 April 2018)

ML and WW v Germany App nos 60798/10 and 65599/10 (ECtHR, 28 June 2018)

Catt v United Kingdom App no 43514/15 (ECtHR, 24 January 2019)

Beizaras and Levickas v. Lithuania App no. 41288/15 (ECtHR, 14 January 2020)

Gaughran v United Kingdom App no 45245/15 (ECtHR, 13 February 2020)

N.Š. v Croatia App no 36908/13 (ECtHR, 10 September 2020)

Liebscher v Austria App no 5434/17 (ECtHR, 6 March 2021)

2.3. Other cases

Prince Albert v Strange (1849) 1 Mac & G(25) 1171

Dumas c Liébert (1867)

McGee v Attorney General [1973] Irish Reports 284

Kennedy v Attorney General [1987] IR 587

3. SCHOLARLY WORKS

Adams-Prassl J, Binns R and Kelly-Lyth A, 'Directly Discriminatory Algorithms' (2022) 86 The Modern Law Review 144

Albrechtslund A, 'Online Social Networking as Participatory Surveillance' (2008) 13 First Monday <https://firstmonday.org/article/view/2142/1949> accessed 7 May 2020

Allen AL, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield 1988)

——, *Unpopular Privacy: What Must We Hide?* (Oxford University Press 2011)

Andrejevic M, 'The Work of Watching One Another: Lateral Surveillance, Risk, and Governance' (2002) 2 Surveillance & Society <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3359> accessed 13 February 2020

Argyrou A and Hummels H, 'Legal Personality and Economic Livelihood of the Whanganui River: A Call for Community Entrepreneurship' (2019) 44 Water International 752

Ausloos J, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection* (Oxford University Press 2020)

Ausloos J and Dewitte P, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4

Azoulai L, 'The European Individual and Collective Entities' in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016)

Azoulai L, Barbou des Places S and Pataut E (eds), *Constructing the Personal in EU Law: Rights, Roles, and Identities* (Hart Publishing 2016)

Azoulai L, Pataut E and Barbou des Places S, 'Being a Person in the European Union' in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016)

Ball K, Di Domenico M and Nunan D, 'Big Data Surveillance and the Body-Subject' (2016) 22 Body & Society 58

Bamberger KA and Mayse AE, 'Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age' (2021) 36 Journal of Law and Religion 495

Bannerman S, 'Relational Privacy and the Networked Governance of the Self' (2019) 22 Information, Communication & Society 2187

Barclay L, 'Autonomy and the Social Self' in Catriona MacKenzie and Natalie Stoljar (eds), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000)

Barnard-Wills D, *Surveillance and Identity: Discourse, Subjectivity and the State* (Ashgate Publishing Ltd 2012)

Barocas S and Levy K, 'Privacy Dependencies' (2020) 95 Washington Law Review 555

Barocas S and Nissenbaum H, ‘Big Data’s End Run around Anonymity and Consent’ in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014)

Barocas S and Selbst AD, ‘Big Data’s Disparate Impact’ (2016) 104 California Law Review 671

Benjamin R, *Race after Technology : Abolitionist Tools for the New Jim Code* (Polity Press 2019)

Berg C, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (Springer Nature Switzerland AG 2018)

Bergemann B, ‘The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection’ in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution*, vol 526 (Springer International Publishing 2018) <http://link.springer.com/10.1007/978-3-319-92925-5_8> accessed 25 August 2021

Bergen M and Surane J, ‘Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales’ *Bloomberg* (30 August 2018) <https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales> accessed 6 March 2019

Bernal P, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014)

Beyleveld D and Brownsword R, *Consent in the Law* (Hart Publishing 2007)

Biczók G and Chia PH, ‘Interdependent Privacy: Let Me Share Your Data’ in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security*, vol 7859 (Springer Berlin Heidelberg 2013) <http://link.springer.com/10.1007/978-3-642-39884-1_29> accessed 23 September 2021

Bieker F, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*, vol 34 (TMC Asser Press 2022)

Bietti E, ‘The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond’ [2020] Hoover Institution Aegis Paper Series 16

Birhane A, ‘Descartes Was Wrong: “A Person Is a Person through Other Persons” | Aeon Ideas’ (*Aeon*, 7 April 2017) <https://aeon.co/ideas/descartes-was-wrong-a-person-is-a-person-through-other-persons> accessed 7 September 2021

Bloustein EJ, ‘Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser’ (1964) 39 New York University Law Review 962

——, ‘Group Privacy: The Right to Huddle’ (1977) 8 Rutgers Camden Law Journal 218

Blume P, ‘The Data Subject’ (2015) 1 European Data Protection Law Review 258

boyd d, ‘Networked Privacy’ (2012) 10 Surveillance & Society 348

Boyle J, ‘Is Subjectivity Possible - The Post-Modern Subject in Legal Theory’ (1991) 62 University of Colorado Law Review 489

Braun V and Clarke V, ‘Using Thematic Analysis in Psychology’ (2006) 3 Qualitative Research in Psychology 77

Bridges K, ‘Privacy Rights and Public Families’ (2011) 34 Harvard Journal of Law and Gender 113

Brkan M, ‘The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning’ (2019) 20 German Law Journal 864

Browne S, *Dark Matters: On the Surveillance of Blackness* (Duke University Press 2015)

Brownsword R, ‘The Cult of Consent: Fixation and Fallacy’ (2004) 15 King’s Law Journal 223

——, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

Brożek B, ‘The Troublesome “Person”’ in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Bugaric B, ‘The Neo-Liberal Bias of the EU Constitutional Order: A Critical Analysis’ in Mark Tushnet and Dimitry Kochenov, *Research Handbook on the Politics of Constitutional Law* (Edward Elgar Forthcoming) <https://www.ssrn.com/abstract=4353114> accessed 20 February 2023

Butin D, Chicote M and Le Métayer D, ‘Strong Accountability: Beyond Vague Promises’, in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Bygrave LA, ‘Data Protection Pursuant to the Right to Privacy in Human Rights Treaties’ (1998) 6 International Journal of Law and Information Technology 247

——, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002)

——, ‘The Body as Data? Biobank Regulation via the “Back Door” of Data Protection Law’ (2010) 2 Law, Innovation and Technology 1

——, ‘Article 4(11). Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles* (Oxford University Press 2021) <https://www.ssrn.com/abstract=3839645> accessed 16 November 2021

——, ‘Data Protection by Design and by Default’ [2022] Oxford Online Encyclopaedia of European Union Law <https://ssrn.com/abstract=3944535>

Bygrave LA and Schartum DW, ‘Consent, Proportionality and Collective Power’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

Bygrave LA and Tosoni L, ‘Article 4(1). Personal Data’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 4(11). Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Calo R, ‘Privacy, Vulnerability, and Affordance’ in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (1st edn, Cambridge University Press 2018) <https://www.cambridge.org/core/product/identifier/9781316831960%23CN-bp-11/type/book_part> accessed 27 January 2022

Campbell FA, ‘“Disability’s” Date with Ontology and the Ableist Body of the Law’ (2001) 10 Griffith Law Review 42

Castelluccia C, ‘Behavioural Tracking on the Internet: A Technical Perspective’ in Serge Gutwirth and others (eds), *European Data Protection: In Good health?* (Springer Netherlands 2012)

Cavoukian A, Dix A and El Emam K, ‘The Unintended Consequences of Privacy Paternalism’ (Information and Privacy Commissioner, Canada 2014)

Chalmers D, ‘The Unconfined Power of European Union Law’ (2016) 1 European Papers 405

——, ‘Informational Self-Determination, EU Law and Informational Capitalism’ (Centre for European Legal Studies Webinar, 27 January 2021) <https://www.youtube.com/watch?v=_TaFB78yt7A> accessed 16 February 2021

Chen J, ‘The Dangers of Accuracy’ (2018) 4 European Data Protection Law Review 36

——, ‘Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption’ (2020) 10 International Data Privacy Law 279

Chesterman S, ‘Artificial Intelligence and the Limits of Legal Personality’ (2020) 69 International and Comparative Law Quarterly 819

Choudary SP, ‘The Rise of Social Graphs for Businesses’ [2015] *Harvard Business Review* <https://hbr.org/2015/02/the-rise-of-social-graphs-for-businesses> accessed 21 March 2019

Christman J, ‘Autonomy’ in Roger Crisp (ed), *The Oxford Handbook of the History of Ethics* (Oxford University Press 2013)

Clifford D, ‘Data Protection and Consumer Protection: The Empowerment of the Citizen Consumer’ in Gloria González Fuster, Rosamunde E Van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022)

Clifford D and Ausloos J, ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130

Cocking D, ‘Plural Selves and Relational Identity: Intimacy and Privacy Online’ in Jeroen van den Hoven and John Weckert (eds), *Information Technology and Moral Philosophy* (Cambridge University Press 2001) <https://www.cambridge.org/core/product/identifier/CBO9780511498725A014/type/book_part> accessed 7 May 2020

Cohen JE, ‘Studying Law Studying Surveillance’ (2014) 13 Surveillance & Society 91

——, ‘The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy’ (2018) 31 Philosophy & Technology 213

——, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019)

——, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1

——, 'Review of Zuboff's The Age of Surveillance Capitalism' (2019) 17 Surveillance & Society 240

Corbyn Z, 'How Taking a Home Genetics Test Could Help Catch a Murderer' *The Observer* (1 December 2018) <https://www.theguardian.com/science/2018/dec/01/how-home-dna-tests-are-solving-cold-cases-golden-state-killer> accessed 21 March 2019

Costa-Cabral F and Lynskey O, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11

Costello RÁ, 'Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?' (2022) 22 Human Rights Law Review ngab031

Couldry N and Mejias UA, *The Costs of Connection : How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019)

Crain M, 'The Limits of Transparency: Data Brokers and Commodification' (2018) 20 New Media & Society 88

Crenshaw KW, 'Race, Reform, and Retrenchment: Transformation and Legitimation in Antidiscrimination Law' (2011) 12 German Law Journal 247

Crowder G, 'Pluralism' in Mark Bevir, *Encyclopedia of Political Theory* (SAGE Publications, Inc 2010) <http://sk.sagepub.com/reference/politicaltheory/n347.xml> accessed 10 September 2020

Curren L and Kaye J, 'Revoking Consent: A "Blind Spot" in Data Protection Law?' (2010) 26 Computer Law & Security Review 273

Dalla Corte L, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 European Journal of Law and Technology 26

——, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data protection and privacy: Data protection and democracy* (Hart Publishing 2020)

Danaher J, Nyholm S and Earp BD, 'The Quantified Relationship' (2018) 18 The American Journal of Bioethics 3

Dani M, 'Assembling the Fractured European Consumer' (2011) 29 LSE 'Europe in Question' Discussion Paper Series <http://www.ssrn.com/abstract=1738474> accessed 1 December 2020

——, 'The Subjectification of the Citizen in European Public Law' (2015) 02 EUI Working Papers 35

Dawson M and Muir E, 'Individual, Institutional and Collective Vigilance in Protecting Fundamental Rights in the EU: Lessons From the Roma' (2011) 48 Common Market Law Review 751

de Brouwer S, ‘Privacy Self-Management and the Issue of Privacy Externalities: Of Thwarted Expectations, and Harmful Exploitation’ (2020) 9 Internet Policy Review <https://policyreview.info/articles/analysis/privacy-self-management-and-issue-privacy-externalities-thwarted-expectations-and> accessed 28 April 2021

de Búrca G, ‘After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?’ (2013) 20 Maastricht Journal of European and Comparative Law 168

De Hert P, ‘Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law’ in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan UK 2012)

de Hert P and Papakonstantinou V, ‘Framing Big Data in the Council of Europe and the EU Data Protection Law Systems: Adding “Should” to “Must” via Soft Law to Address More than Only Individual Harms’ (2021) 40 Computer Law & Security Review 105496

de Hingh A, ‘Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation’ (2018) 19 German Law Journal 1269

de Witte F, ‘Emancipation through Law?’ in Loïc Azoulai, Etienne Pataut and Ségolène Barbou des Places (eds), *Constructing the Person in EU Law: Rights, Roles, Identities* (Hart Publishing 2016)

——, ‘Integrating the Subject: Narratives of Emancipation in Regionalism’ (2019) 30 European Journal of International Law 257

Delacroix S and Lawrence ND, ‘Bottom-up Data Trusts: Disturbing the “One Size Fits All” Approach to Data Governance’ [2019] International Data Privacy Law ipz014

Donovan S, ‘“Sharenting”: The Forgotten Children of the GDPR’ (2020) 4 Peace Human Rights Governance 35

Douzinas C, *The End of Human Rights: Critical Thought at the Turn of the Century* (Bloomsbury Publishing Plc 2000)

——, ‘The Paradoxes of Human Rights’ (2013) 20 Constellations 51

Drechsler L, ‘Did the Court of Justice (Re-)Define the Purpose of the General Data Protection Regulation?’ (*CITIP blog*, 14 February 2023) <https://www.law.kuleuven.be/citip/blog/did-the-court-of-justice-re-define-the-purpose-of-the-general-data-protection-regulation/> accessed 20 February 2023

Dupré C, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Bloomsbury Publishing Plc 2015)

Easley D and Ghosh A, ‘Incentives, Gamification, and Game Theory: An Economic Approach to Badge Design’ (2016) 4 ACM Transactions on Economics and Computation 1

Edwards L and others, ‘Data Subjects as Data Controllers: A Fashion(Able) Concept?’ (*Internet Policy Review*) <https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400> accessed 21 October 2019

Erdos D, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (Oxford University Press 2019)

——, ‘Comparing Constitutional Privacy and Data Protection Rights within the EU’ (2022) 47 European Law Review 482

Erlich Y and others, ‘Identity Inference of Genomic Data Using Long-Range Familial Searches’ (2018) 362 Science 690

Etzioni A, *Privacy in a Cyber Age: Policy and Practice* (Palgrave Macmillan 2015)

Fabbrini F, ‘The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court’ in Sybe A De Vries, Ulf Bernitz and Stephen Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years On*, vol 20 (Hart Publishing 2015)

Fairfield J and Engel C, ‘Privacy as a Public Good’ (2015) 65 Duke Law Journal 385

Fereday J and Muir-Cochrane E, ‘Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development’ (2006) 5 International Journal of Qualitative Methods 80

Finck M, ‘Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law’ (2021) 11 International Data Privacy Law 333

Floridi L, ‘Open Data, Data Protection, and Group Privacy’ (2014) 27 Philosophy & Technology 1

——, ‘On Human Dignity as a Foundation for the Right to Privacy’ (2016) 29 Philosophy & Technology 307

——, ‘Group Privacy: A Defence and an Interpretation’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017)

Fortin JES, ‘Legal Protection for the Unborn Child’ (1988) 51 The Modern Law Review 54

Foster C and Herring J, *Identity, Personhood and the Law* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-53459-6> accessed 10 August 2020

Fuchs C, ‘Towards an Alternative Concept of Privacy’ (2011) 9 Journal of Information, Communication and Ethics in Society 220

Galetta A, Fonio C and Ceresa A, ‘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”’ [2015] International Data Privacy Law ipv026

Gandy OH and Nemorin S, ‘Toward a Political Economy of Nudge: Smart City Variations’ (2019) 22 Information, Communication & Society 2112

Gellert R, ‘Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative’ (2015) 5 International Data Privacy Law 3

——, *The Risk-Based Approach to Data Protection* (1st edn, Oxford University Press 2020)

Gellert R and Gutwirth S, ‘The Legal Construction of Privacy and Data Protection’ (2013) 29 Computer Law & Security Review 522

Gentile G and Lynskey O, ‘Deficient by Design? The Transnational Enforcement of the GDPR’ (2022) 71 International and Comparative Law Quarterly 799

Georgieva L and Kuner C, ‘Article 9. Processing of Special Categories of Personal Data’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Gil González E and de Hert P, ‘Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles’ (2019) 19 ERA Forum 597

Glenn HP, ‘A Civil Law Tradition: The Centrality of The Person’, *Legal Traditions of the World: Sustainable diversity in Law* (5th edn, Oxford University Press 2014) <https://doi.org/10.1093/he/9780199669837.003.0005>

González Fuster G, ‘Fighting For Your Right to What Exactly - The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection’ (2014) 2 Birbeck Law Review 263

——, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014)

——, ‘Article 80. Representation of Data Subjects’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Gotanda N, ‘A Critique of “Our Constitution Is Color-Blind”’ (1991) 44 Stanford Law Review 1

Graziadei M, ‘Rights in the European Landscape: A Historical and Comparative Profile’ in Sacha Prechal and Bert van Roermund, *The Coherence of EU Law: The Search for Unity in Divergent Concepts* (Oxford University Press 2008)

Greenleaf G, ‘The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108?’ (2012) 12 University of Edinburgh Research Paper Series 36

——, ‘“European” Data Privacy Standards Implemented in Laws Outside Europe’ (2018) 18 University of New South Wales Law Research Series <https://ssrn.com/abstract=3096314> accessed 9 April 2019

Gutwirth S and De Hert P, ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in Serge Gutwirth and others (eds), *Reinventing data protection?* (Springer 2009)

Hamari J, Hassan L and Dias A, ‘Gamification, Quantified-Self or Social Networking? Matching Users’ Goals with Motivational Technology’ (2018) 28 User Modeling and User-Adapted Interaction 35

Harlow C, ‘“Public” and “Private” Law: Definition Without Distinction’ (1980) 43 The Modern Law Review 241

Hartzog W, ‘Opinions · The Case Against Idealising Control’ (2018) 4 European Data Protection Law Review 423

Helberger N and Hoboken J van, ‘Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers’ (2010) 11 Computer Law Review International 101

Helberger N, Zuiderveen Borgesius FJ and Reyna A, ‘The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law’ (2017) 54 Common Market Law Review 1427

Hermida A and Hernández-Santaolalla V, ‘Horizontal Surveillance, Mobile Communication and Social Networking Sites. The Lack of Privacy in Young People’s Daily Lives’ (2020) 33 Communication & Society 139

Herring J, ‘Forging a Relational Approach: Best Interests or Human Rights?’ (2013) 13 Medical Law International 32

Hildebrandt M, *Smart Technologies and the End(s) of Law* (Edward Elgar Publishing Ltd 2015)

——, ‘Discrimination, Data-Driven AI Systems and Practical Reason’ (2021) 7 European Data Protection Law Review 358

Hirsch DD, ‘Privacy. Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel’ (2016) 65 Duke Law Journal 67

Hornung G and Schnabel C, ‘Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination’ (2009) 25 Computer Law & Security Review 84

Horwitz MJ, ‘The History of the Public/Private Distinction’ (1982) 130 University of Pennsylvania Law Review 1423

Hughes K, ‘The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse’ in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015)

Hull G, Lipford HR and Latulipe C, ‘Contextual Gaps: Privacy Issues on Facebook’ (2011) 13 Ethics and Information Technology 289

Humphreys L, Santos C, di Caro L and Boella, G, ‘Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation’ (2015) JURIX 41.

Hustinx P, ‘EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation’ in Marise Cremona (ed), *New Technologies and EU Law* (Oxford University Press 2017)

Janciute L, ‘Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities’ (2019) 9 International Data Privacy Law 13

Janssen H, Cobbe J and Singh J, ‘Personal Information Management Systems: A User-Centric Privacy Utopia?’ (2020) 9 Internet Policy Review <https://policyreview.info/articles/analysis/personal-information-management-systems-user-centric-privacy-utopia> accessed 13 January 2021

Jones ML, ‘Privacy without Screens & the Internet of Other People’s Things’ [2015] Idaho Law Review 1

Jones P, ‘Human Rights, Group Rights, and Peoples’ Rights’ (1999) 21 Human Rights Quarterly 80

Kaminski ME, ‘The Case for Data Privacy Rights (Or ’Please, a Little Optimism’)’ (2022) 97 Notre Dame Law Review Reflection 385

Kapczynski A, ‘The Law of Informational Capitalism’ [2020] The Yale Law Journal 1460

Kennedy D, ‘The International Human Rights Movement: Part of the Problem?’ in Robert McCorquodale (ed), Robert McCorquodale, *Human Rights* (1st edn, Routledge 2017)

Kirkland AR, *Fat Rights: Dilemmas of Difference and Personhood* (New York University Press 2008)

Klein LF and D’Ignazio C, *Data Feminism* (MIT Press 2020)

Klimas T and Vaitiukait J, ‘The Law of Recitals in European Community Legislation’ (2008) 15 Journal of International & Comparative Law 60

Koivisto J and Hamari J, ‘The Rise of Motivational Information Systems: A Review of Gamification Research’ (2019) 45 International Journal of Information Management 191

Kokott J and Sobotta C, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222

Koops B-J, ‘The Trouble with European Data Protection Law’ (2014) 4 International Data Privacy Law 250

Kosta E, *Consent in European Data Protection Law* (Brill 2013)

——, ‘Article 7. Conditions for Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 8. Conditions Applicable to Child’s Consent in Relation to Information Society Services’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 35. Data Protection Impact Assessment’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Kotschy W, ‘Article 6. Lawfulness of Processing’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Kuner C and others, ‘When Two Worlds Collide: The Interface between Competition Law and Data Protection’ (2014) 4 International Data Privacy Law 247

Kurki VAJ and Pietrzykowski T (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer 2017)

Kuru T and Beriain I de M, ‘Your Genetic Data Is My Genetic Data: Unveiling Another Enforcement Issue of the GDPR’ (2022) 47 Computer Law & Security Review 105752

Lacey N, *Women, Crime, and Character* (Oxford University Press 2008)

Laidlaw EB, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24 International Review of Law, Computers & Technology 263

Lazaro C and Le Métayer D, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 SCRIPTed <http://script-ed.org/?p=1927> accessed 6 November 2018

Levy K, 'Relational Big Data' (2013) 66 Stanford Law Review Online 73

——, 'Intimate Surveillance' (2015) 51 Idaho Law Review 679

——, 'The Phallus-y Fallacy: On Unsexy Intimate Tracking' (2018) 18 The American Journal of Bioethics 22

Levy K and Schneier B, 'Privacy Threats in Intimate Relationships' (2020) 6 Journal of Cybersecurity 1

L'Hoiry X and Norris C, 'The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, vol 34 (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-47573-8> accessed 21 June 2022

Lievens E and Verdoodt V, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 269

Lindroos-Hovinheimo S, 'Private Selves - An Analysis of Legal Individualism' in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer International Publishing 2017)

——, 'There Is No Europe-On Subjectivity and Community in the EU' (2017) 18 German Law Journal 19

——, *Private Selves: Legal Personhood in European Privacy Protection* (Cambridge University Press 2021)

Livingstone S, 'Children: A Special Case for Privacy?' (2018) 46 Intermedia 18

Lodge M and Wegrich K, *Managing Regulation* (Macmillan Education UK 2012) <http://link.springer.com/10.1007/978-1-137-26552-4> accessed 7 January 2022

Lowe EJ, 'Individuation' in Michael J Loux and Dean W Zimmerman (eds), *The Oxford Handbook of Metaphysics* (Oxford University Press 2005) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199284221.001.0001/oxfordhb-9780199284221-e-4> accessed 25 September 2019

Lupton D, 'The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance' (2016) 45 Economy and Society 101

Lynskey O, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Netherlands 2013)

——, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569

——, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

——, ‘The “Europeanisation” of Data Protection Law’ (2017) 19 Cambridge Yearbook of European Legal Studies 252

——, ‘Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy’ (2019) 20 Theoretical Inquiries in Law 189

——, ‘Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing’ (2019) 15 International Journal of Law in Context 162

——, ‘Delivering Data Protection: The Next Chapter’ (2020) 21 German Law Journal 80

——, ‘Extraterritorial Impact in Data Protection Law through an EU Law Lens’ in Federico Fabbrini, Eduardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing 2021) <https://www.ssrn.com/abstract=3674413> accessed 29 October 2020

Macenaite M, ‘From Universal towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation’ (2017) 19 New Media & Society 765

Mackenzie C, ‘Relational Autonomy’ in Kim Q Hall and Ásta (eds), Catriona Mackenzie, *The Oxford Handbook of Feminist Philosophy* (Oxford University Press 2021)

MacKinnon CA, *Toward a Feminist History of the State* (Harvard University Press 1989)

Maclean A, *Autonomy, Informed Consent and Medical Law: A Relational Challenge* (Cambridge University Press 2009) <http://ebooks.cambridge.org/ref/id/CBO9780511576119> accessed 16 September 2021

Mahieu R, ‘The Right of Access to Personal Data: A Genealogy’ [2021] Technology and Regulation 62

Mahieu R, van Hoboken J and Asghari H, ‘Responsibility for Data Protection in a Networked World – On the Question of the Controller, “Effective and Complete Protection” and Its Application to Data Access Rights in Europe’ (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 39

Mai J-E, ‘Big Data Privacy: The Datafication of Personal Information’ (2016) 32 The Information Society 192

Malgieri G and Niklas J, ‘Vulnerable Data Subjects’ (2020) 37 Computer Law & Security Review 105415

Mansfield N, *Subjectivity: Theories of the Self from Freud to Haraway* (New York University Press 2000)

Mantelero A, ‘Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection’ (2016) 32 Computer Law & Security Review 238

Marks S, ‘Four Human Rights Myths’ in David Kinley, Wojciech Sadurski and Kevin Walton (eds), *Human rights: Old Problems, New Possibilities* (Edward Elgar Publishing Ltd 2013)

Marx GT, ‘Coming to Terms: The Kaleidoscope of Privacy and Surveillance’, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015)

Mason D and Raab CD, 'Privacy, Surveillance, Trust and Regulation: Individual and Collective Dilemmas of Online Privacy Protection' (2002) 5 Information, Communication & Society 379

Matzner T and others, 'Do-It-Yourself Data Protection—Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move*, vol 24 (Springer Netherlands 2016) <http://link.springer.com/10.1007/978-94-017-7376-8_11> accessed 21 March 2019

Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Philip E Agre and Marc Rotenberg, *Technology and privacy: the new landscape* (MIT Press 1997)

Mayer-Schönberger V and Cukier K, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Mariner Books 2014)

McCahill M and Finn RL, *Surveillance, Capital and Resistance: Theorizing the Surveillance Subject* (Routledge 2015)

Mejias UA and Couldry N, 'Datafication' (2019) 8 Internet Policy Review <https://policyreview.info/concepts/datafication> accessed 25 July 2022

Merry SE, 'Relating to the Subjects of Human Rights: The Culture of Agency in Human Rights Discourse' in Michael Freeman and David Napier (eds), *Law and Anthropology* (Oxford University Press 2009)

Mittelstadt B, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475

Monahan T and Murakami Wood D, 'Surveillance Studies as a Transdisciplinary Endeavor' in Torin Monahan and David Murakami Wood (eds), *Surveillance Studies: A Reader* (Oxford University Press 2018)

Moore A, 'Defining Privacy' (2008) 39 Journal of Social Philosophy 411

Moser I, 'Disability and the Promises of Technology: Technology, Subjectivity and Embodiment within an Order of the Normal' (2006) 9 Information, Communication & Society 373

Muir E, 'Of Ages In-and Edges Of-EU Law' (2011) 48 Common Market Law Review 39

——, 'The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges' (2014) 51 Common Law Market Review 219

Mulligan A, 'Maternal Brain Death and Legal Protection of the Foetus in Ireland' (2015) 15 Medical Law International 182

Nadler A and McGuigan L, 'An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing' (2018) 35 Critical Studies in Media Communication 151

Naffine N, 'Legal Persons as Abstractions: The Extrapolation of Persons from the Male Case' in Visa AJ Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Nedelsky J, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (Oxford University Press 2011)

Ní Loideáin N, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

——, 'A Port in the Data-Sharing Storm: The GDPR and the Internet of Things' (2019) 4 Journal of Cyber Policy 178

Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

Noble SU, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018)

Nolan K, 'Book Review: Private Selves: Legal Personhood in European Privacy Protection' (2021) 7 European Data Protection Law Review 624

O'Brien C, 'I Trade, Therefore I Am: Legal Personhood in the European Union' (2013) 50 Common Market Law Review 1643

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701

Oostveen M, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 International Data Privacy Law 299

Ostrom E, 'Collective Action and the Evolution of Social Norms' (2000) 14 Journal of Economic Perspectives 137

Ouald Chaib S, 'Procedural Fairness as a Vehicle for Inclusion in the Freedom of Religion Jurisprudence of the Strasbourg Court' (2016) 16 Human Rights Law Review 483

Pagallo U, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017)

Panagiotopoulos A, 'Genetic Information and Communities: A Triumph of Communitarianism over the Right to Data Protection under the GDPR?' (2018) 4 European Data Protection Law Review 459

Peers S and Prechal S, 'Article 52 - Scope and Interpretation of Rights and Principles' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights: a commentary (2nd edn, Bloomsbury Publishing Plc 2021);

Peifer K-N and Schwartz PM, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115

Perrot M and Guerrand R-H, 'Scenes and Places' in Michelle Perrot (ed), Arthur Goldhammer (tr), *A History of Private Life: From the Fires of Revolution to the Great War*, vol 4 (Harvard University Press 1990)

Piasecki S and Chen J, ‘Complying with the GDPR When Vulnerable People Use Smart Devices’ [2022] International Data Privacy Law ipac001

Porcedda MG, ‘On Boundaries-Finding the Essence of the Right to the Protection of Personal Data’ in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019)

Prosser WL, ‘Privacy’ (1960) 48 California Law Review 383

Purtova N, ‘Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table … and Back on Again?’ (2014) 30 Computer Law & Security Review 6

——, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10 Law, Innovation and Technology 40

——, ‘From Knowing by Name to Targeting: The Meaning of Identification under the GDPR’ [2022] International Data Privacy Law ipac013

Quelle C, ‘Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection’ in Anja Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps*, vol 498 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-55783-0_11> accessed 3 August 2021

Quinn P and Quinn L, ‘Big Genetic Data and Its Big Data Protection Challenges’ (2018) 34 Computer Law & Security Review 1000

Reed C, ‘The Law of Unintended Consequences – Embedded Business Models in IT Regulation’ [2007] Journal of Information, Law and Technology 33

Reed C and Murray A, *Rethinking the Jurisprudence of Cyberspace* (Edward Elgar Publishing 2018)

Regan PM, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press 1995)

——, ‘Privacy as a Common Good in the Digital World’ (2002) 5 Information, Communication & Society 382

Reviglio U and Alunge R, ‘“I Am Datafied Because We Are Datafied”: An Ubuntu Perspective on (Relational) Privacy’ (2020) 33 Philosophy & Technology 595

Richards N and Hartzog W, ‘A Relational Turn for Data Protection?’ (2020) 4 European Data Protection Law Review 1

Richardson M, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press 2017)

Roessler B, *The Value of Privacy* (Polity Press 2001)

Rott P, ‘Data Protection Law as Consumer Law – How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law’ (2017) 3 Journal of European Consumer and Market Law 113

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Sacharoff L, 'The Relational Nature of Privacy' (2012) 16 Lewis & Clark Law Review 1249

Sætra HS, 'Privacy as an Aggregate Public Good' (2020) 63 Technology in Society 101422

Schoeman FD, 'The Meaning and Scope of Privacy', *Privacy and Social Freedom* (Cambridge University Press 1992)

Scholz LH, 'Private Rights of Action in Privacy Law' (2022) 63 William and Mary Law Review 58

Schwartz PM, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review; Nashville 1609

Schwartz PM and Peifer K-N, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?' (2010) 98 California Law Review 64

——, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 65

Scudder N and others, 'Policy and Regulatory Implications of the New Frontier of Forensic Genomics: Direct-to-Consumer Genetic Data and Genealogy Records' (2019) 31 Current Issues in Criminal Justice 194

Shildrick M, *Dangerous Discourses of Disability, Subjectivity and Sexuality* (Palgrave Macmillan 2009)

Siedentop L, *Inventing the Individual: The Origins of Western Liberalism* (Penguin Books 2014)

Sipior JC, Ward BT and Mendoza RA, 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons' (2011) 10 Journal of Internet Commerce 1

Skinner-Thompson S, *Privacy at the Margins* (Cambridge University Press 2021)

Smuha NA, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review <https://policyreview.info/articles/analysis/beyond-individual-governing-ais-societal-harm> accessed 7 December 2021

Snyder TJ, 'Developing Privacy Rights in Nineteenth-Century Germany: A Choice between Dignity and Liberty?' (2018) 58 American Journal of Legal History 188

Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087

——, *Understanding Privacy* (Harvard University Press 2008)

——, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880

——, 'The Meaning and Value of Privacy', *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015)

Somek A, *Individualism: An Essay on the Authority of the European Union* (Oxford University Press 2008)

——, ‘European Constitutionalism: The Neoliberal Drift’ (*LPE Project*, 11 April 2019) <https://lpeproject.org/blog/european-constitutionalism-the-neoliberal-drift/> accessed 20 February 2023

Stucke ME and Grunes AP, *Big Data and Competition Policy* (Oxford University Press 2016)

Sunstein CR, ‘Requiring Choice Is a Form of Paternalism’ (2017) 1 Journal of Behavioral Economics for Policy 11

Susser D, Roessler B and Nissenbaum H, ‘Technology, Autonomy, and Manipulation’ (2019) 8 Internet Policy Review <https://policyreview.info/node/1410> accessed 10 September 2020

Symeonidis I and others, ‘Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence’ in Jaap-Henk Hoepman and Stefan Katzenbeisser (eds), *ICT Systems Security and Privacy Protection*, vol 471 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-33630-5_14> accessed 23 September 2021

Taylor C, *Sources of the Self: The Making of the Modern Identity* (Cambridge University Press 1989)

Taylor L, Floridi L and van der Sloot B (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-46608-8> accessed 2 December 2020

——, ‘Introduction: A New Perspective on Privacy’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (Springer International Publishing 2017)

ten Haaf L, ‘Unborn and Future Children as New Legal Subjects: An Evaluation of Two Subject-Oriented Approaches—The Subject of Rights and the Subject of Interests’ (2017) 18 German Law Journal 1091

Thomas J, *Public Rights, Private Relations* (Oxford University Press 2015)

Thomas K, Grier C and Nicol DM, ‘UnFriendly: Multi-Party Privacy Risks in Social Networks’ in Mikhail J Atallah and Nicholas J Hopper (eds), *Privacy Enhancing Technologies*, vol 6205 (Springer Berlin Heidelberg 2010) <http://link.springer.com/10.1007/978-3-642-14527-8_14> accessed 23 September 2021

Trnka S and Trundle C, ‘Competing Responsibilities: Moving Beyond Neoliberal Responsibilisation’ (2014) 24 Anthropological Forum 136

Trotter SJ, ‘On Coming to Terms: How European Human Rights Law Imagines the Human Condition’ (Doctor of Philosophy, The London School of Economics and Political Science 2018) <http://etheses.lse.ac.uk/3946/1/Trotter__On-coming-terms-European-human-rights.pdf>

Turkel G, ‘The Public/Private Distinction: Approaches to the Critique of Legal Ideology’ (1988) 22 Law and Society Review 807

Van Alsenoy B, ‘Allocating Responsibility among Controllers, Processors, and “Everything in between”: The Definition of Actors and Roles in Directive 95/46/EC’ (2012) 28 Computer Law & Security Review 25

——, ‘The Evolving Role of the Individual under EU Data Protection Law’ [2015] CiTiP Working Paper Series 36

——, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia Ltd 2019)

Van Bekkum M and Zuiderveen Borgesius F, ‘Using Sensitive Data to Prevent Discrimination by AI: Does the GDPR Need a New Exception?’ (2022) 48 Computer Law & Security Review 105770

——, ‘Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation’ (2014) 4 International Data Privacy Law 307

Sloot B van der, *Privacy as Virtue: Moving beyond the Individual in the Age of Big Data* (Intersentia 2017)

Van Dijck J, ‘Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology’ (2014) 12 Surveillance & Society 197

Vedder A, ‘KDD: The Challenge to Individualism’ (1999) 1 Ethics and Information Technology 275

Venkatadri G and others, ‘Auditing Offline Data Brokers via Facebook’s Advertising Platform’, *The World Wide Web Conference* (ACM 2019) <https://dl.acm.org/doi/10.1145/3308558.3313666> accessed 12 March 2023

Viljoen S, ‘Democratic Data: A Relational Theory For Data Governance’ (2021) 131 Yale Law Journal 573

Volpp L, ‘The Citizen and the Terrorist’ in Cyra Akila Choudhury and Khaled A Beydoun (eds), *Islamophobia and the Law* (1st edn, Cambridge University Press 2020) <https://www.cambridge.org/core/product/identifier/9781108380768%23CN-bp-1/type/book_part> accessed 21 February 2023

Wachter S, ‘Affinity Profiling and Discrimination By Association in Online Behavioral Advertising’ (2020) 35 Berkeley Technology Law Journal 367

Wachter S and Mittelstadt B, ‘A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI’ (2018) 1 Columbia Business Law Review <https://osf.io/mu2kf> accessed 3 May 2019

Wagner WJ, ‘The Development of the Theory of the Right to Privacy in France’ [1971] Washington University Law Review 28

Wahrman D, *The Making of the Modern Self: Identity and Culture in Eighteenth-Century England* (Yale University Press 2004)

Waldau P, ‘Animals as Legal Subjects’ in Linda Kalof (ed), Paul Waldau, *The Oxford Handbook of Animal Studies* (Oxford University Press 2017) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199927142.001.0001/oxfordhb-9780199927142-e-13> accessed 13 May 2022

Walden IN and Savage RN, ‘Data Protection and Privacy Laws: Should Organisations Be Protected?’ (1988) 37 International and Comparative Law Quarterly 337.

Waldman AE, ‘Privacy’s Rights Trap’ (2022) 117 Northwestern University Law Review 88

——, ‘Privacy, Practice, and Performance’ (2022) 110 California Law Review 1221

Warin C, ‘Individual Rights and Collective Interests in EU Law: Three Approaches to a Still Volatile Relationship’ (2019) 56 Common Market Law Review 463

Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193

Weiler JHH, ‘Van Gend En Loos: The Individual as Subject and Object and the Dilemma of European Legitimacy’ (2014) 12 International Journal of Constitutional Law 94

Weinberg L, ‘Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden’ (2017) 12 Westminster Papers in Culture and Communication 5

Westin AF, *Privacy and Freedom* (2018th edn, Ig Publishing 1967)

Whitman JQ, ‘The Two Western Cultures of Privacy: Dignity Versus Liberty’ The Yale Law Journal 1153

Williams PJ, ‘Alchemical Notes: Reconstructing Ideals from Deconstructed Rights’ (1987) 22 Harvard Civil Rights-Civil Liberties Law Review, 401

——, *The Alchemy of Race and Rights* (Harvard University Press 1991)

de Witte B, ‘Article 53 - Level of Protection’ in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights: a commentary (2nd edn, Bloomsbury Publishing Plc 2021)

Wise SM, ‘Legal Personhood and the Nonhuman Rights Project’ (2010) 17 Animal Law 1

Wojtczak S, ‘Endowing Artificial Intelligence with Legal Subjectivity’ (2022) 37 AI & Society 205

Wong B, ‘Delimiting the Concept of Personal Data after the GDPR’ (2019) 39 Legal Studies 517

Wong J, Henderson T and Ball K, ‘Data Protection for the Common Good: Developing a Framework for a Data Protection-Focused Data Commons’ (2022) 4 Data & Policy e3

Zanfir G, ‘Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law’ in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Zuboff S, ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30 Journal of Information Technology 75

——, *The Age of Surveillance Capitalism* (Profile Books Ltd 2019)