University of Hertfordshire UH

Research Archive

Citation for published version:
Henry Pearce, ‘Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?’, *Information & Communications Technology Law,* Vol. 27 (2): 133-165, April 2018.

DOI:
https://doi.org/10.1080/13600834.2018.1458449

Document Version:
This is the Accepted Manuscript version.
The version in the University of Hertfordshire Research Archive may differ from the final published version.

Copyright and Reuse:
© 2018 Informa UK Limited, trading as Taylor & Francis Group

Content in the UH Research Archive is made available for personal research, educational, and non-commercial purposes only. Unless otherwise stated, all content is protected by copyright, and in the absence of an open license, permissions for further re-use should be sought from the publisher, the author, or other copyright holder.

Enquiries
If you believe this document infringes copyright, please contact Research & Scholarly Communications at rsc@herts.ac.uk

Title

Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?

Henry Pearce, University of Hertfordshire, Lecturer in Law

Hertfordshire Law School

University of Hertfordshire,

Hatfield,

Hertfordshire,

AL10 9EU

Email: h.pearce@herts.ac.uk

Keywords:

Data protection, moral rights, control, personal data, individual rights.

Abstract:

This article considers the notion of individual control of personal data as envisaged by the European data protection framework and makes the argument that it is a poorly-understood and under-developed concept, but that our understanding of it may be improved by way of analyses and comparisons with the doctrine of moral rights, an important constituent element of intellectual property law. The article starts by examining the concept of personal data itself, and why an enhanced level of individual control over personal data is thought to be a desirable regulatory objective. Following this, the article examines the scholarly literature pertaining to individual control of personal data, as well as a range of relevant EU policy documents. Having done so, the article argues that the notion of control is muddled and confused from both theoretical and practical perspectives. Following this, the article considers the doctrine of moral rights, and through an exploration of its theoretical and practical elements highlights why it may be of assistance in terms of enhancing our understanding of individual control in the data protection context.

In recent years there has been an observable increase in appetite for the establishment and affirmation of regulatory and legal rules that aim to provide individuals with greater control over their personal data. The drive behind this increase in appetite appears to be the underlying belief that ensuring individual control over personal data represents one significant potential way through which increased levels of individual privacy and data protection can be achieved, and by which levels of trust in digital environments and online services can be enhanced. However, despite references to individual control of personal data becoming increasingly prominent in EU policy documents, academic literature, and other sources, the true meaning and normative character of control in this context appears indistinct and seemingly under-studied.

Particularly, in light of recent technological developments and the concurrent emergence of new social practices, questions that are in need of address, but to date appear to have been answered inconclusively, include: what does it really mean to control one's data in relation to contemporary data handling and processing activities? What are the underlying purposes of this control? What are the scope and limits of this control? How can this control be achieved? And, what role should the law play in establishing that control?

Given that the disclosure, and subsequent processing, of personal data has become a fundamental feature of contemporary day to day life, it is important that we engage with these questions to develop a more rigorous understanding of the notion of control in the context of the European data protection framework to prevent it from becoming a hollow and vacuous notion, and so that its pragmatic elements can be fully realised. The aim of this article is to examine the notion of individual control of personal data as envisaged by European data protection law and policy, highlight its possible ambiguities and lack of precision, and consider whether our understanding of control in this context might be enhanced by way of comparisons that can be made with the doctrine of moral rights, an important aspect of intellectual property law.

To this end, the paper takes the following structure. First, the notion of personal data, the key enabling concept of the European data protection framework, is considered, along with why it is thought that an increased level of individual control over personal data is thought to be a desirable regulatory objective. Second, an overview of scholarly and academic literature pertaining to the notion of individual control of personal data and information is provided. Third, by way of an examination of legislative instruments and associated policy documents, the article examines the notion of individual control as contained within the European data protection framework. Having made the case that in the context of the European data protection framework control is a poorly-understood and under-developed concept, the article then turns its attentions to the doctrine of moral rights, a key constituent area of intellectual property law. Through an examination of the theoretical underpinnings of the doctrine of moral rights, and the implementation of the doctrine's implementation in the law of the United Kingdom, the article tentatively concludes that despite intellectual property and data protection law initially seeming prima facie qualitatively different, possibly and mismatched, areas of legal scholarship, our understanding of the notion of individual control as contained within the European data protection framework may well benefit from further comparisons and analyses between the two disciplines.

1. Personal data

Before examining the substantive provisions of the European data protection framework pertaining to individual control it is first important to have an appreciation of data protection law's key enabling concept, personal data itself, and precisely why it is there is a growing appetite to establish individual

control over it. At the time of writing, the European Union's main legislative instrument in the data protection framework is the Data Protection Directive,[1] which defines personal data as:

> *"…any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*"[2]

The General Data Protection Regulation, which has been drafted as a means of bringing the data protection framework into line with contemporary data-handling practices and will replace the Directive and apply in all EU Member States from May 2018,[3] provides an updated version of the Directive's earlier definition:

> *"…any information relating to an identified or identifiable natural person 'data subject'; an identifiable 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, online identifier or to one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of that person;"*[4]

The notion of personal data under both legislative instruments is, therefore, very broad, and includes, by way of example, the following types of data: Identifying data of an official nature, such as name, financial information, and health information; demographic data, including age, race, gender, income, sexual preferences and political affiliations; activity or behavioural data, including internet search and browsing histories, and records of commercial transactions; locational data and internet protocol addresses; and social data, including contacts and friends on social networking sites.

Personal data of all these types have progressively become central to the activities of public-sector organisations and to the business models of a wealth of private companies, particularly those operating online, many of which rely on the collection of the personal data of their users to accrue capital. Providers of search engine services, mobile applications, online shops and social media platforms represent some notable examples of such companies. When individuals make use of services of this sort, personal data of all the above-mentioned types will habitually be collected in several ways.

Primarily, personal data can be *volunteered* or *surrendered* by individuals through them explicitly sharing information about themselves (e.g. when they create a profile on a social networking site or mobile application, enter credit card information so to make a payment, provide personal information as a condition of registration to an online service, or post information about themselves on a forum or blog). Additionally, personal data can be *observed* by recording the activities of individuals, in contrast to the data they provide voluntarily (e.g. an individual's internet browsing preferences, location data, search engine history, app use history). Finally, personal data can be *inferred*, based on the analysis of personal data collected under the previous two headings, or from data collected from other sources (e.g. location data, search engine history, and browsing behaviours can be used as a basis for sophisticated consumer profiling processes, and credit scores can be calculated on the basis of several pieces of

---

[1] Officially known as 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. [Hereinafter the Data Protection Directive]

[2] *Ibid*., Article 2 (a).

[3] An agreed text of the General Data Protection Regulation was adopted by the European Parliament in April 2016, bringing four years of negotiations on the overhaul of European data protection rules to a close. See: European Parliament (2016) "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era (last accessed December 2017)

[4] General Data Protection Regulation, Article 4 (1)

personal data or other seemingly anonymous or pseudonymous data).[5] Increasingly, the latter two categories are becoming integral to the processes of many actors operating in digital environments. This is especially true in respect of institutions and firms who engage in big data analytics, many of which will use observed or inferred personal data to profile individuals so to make inferences about their character, usually as a basis for increasingly sophisticated targeted marketing endeavours.

Personal data that are collected in any of these ways, however, will usually be processed by the collecting third party, on servers under the third party's control, to which the individual to whom those data relate will have no access and will not be able to directly influence. This is problematic, as it is now widely recognised that many of the data processing activities undertaken by such institutions can potentially lead to harmful consequences for the individuals whose personal data are involved, such as breaches of individual privacy and data protection, or possibly discriminatory treatment.[6]

As a corollary of this, and as is explained below, it is now increasingly being suggested that the development of user-centric models of data protection, under which individuals can exercise greater control of their personal data, so to prevent those data from being acquired by illicit third parties, or used for illegitimate or harmful purposes, is a promising way through which any undesirable consequences associated with the processing of personal data in contemporary digital environments can be guarded against. At the same time, it is also hoped that doing so will help build trust between individuals and the parties that seek their personal data. This, it is thought, will help develop economic uses of data and assist with the completion of initiatives like the EU's Digital Market Strategy.[7] Whilst discussions of the notion of control in the context of laws pertaining to data protection, privacy and the control of certain types of information or data are nothing new, it is for these reasons that they are now perhaps more prominent than at any previous point in time.

2. Scholarly approaches to individual control of personal data and information

As suggested above, in recent years the notion of individual control of personal data has become increasingly prominent in the academic literature pertaining to both privacy and data protection. This, however, should not necessarily be considered a novel development. Debates over individual control of personal data have, in fact, over the course of the last one hundred or so years at least, formed the basis

---

[5] OECD (2013) "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No.220, OECD Publishing. pg.10. To underline the potential in the analysis of pseudonymous data a recent study by de Montjoye, et al, on inferred mobile data showed that four spatio-temporal points are enough to uniquely identify 95% of individuals. de Montjoye, Y. et al. (2013) "Unique in the Crowd: The privacy bounds of human mobility", *Scientific Reports* 3. Earlier, in 2009, Ohm identified that pseudonymous and anonymous data can often easily be de-anonymised, partially or entirely, allowing for specific individuals to be identified. Ohm, P. (2009) "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review* 57.

[6] Bevitt, A. and Dietschy, L. (2016) "GDPR series: the risks with data profiling", *Privacy and Data Protection*; Cohen, J. (2013) "What Privacy Is For", *Harvard Law Review 1904*, pp.1918-1927; Taddicken, M. "Privacy, Surveillance, and Self-Disclosure in the Social Web: Exploring the user's Perspective in Focus Groups", Fuchs, C. in *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, ed. by Fuchs, C. et al. (2011) New York: Routledge, pg.266.

[7] European Commission (last accessed December 2017) "Digital Single Market: Digital Economy & Society", https://ec.europa.eu/digital-single-market/en/digital-single-market; Recent research undertaken in the UK by the Information Commissioner's Office and the BLAH GB Group has suggested that individuals increasingly desire greater transparency and control in respect of how their personal data are collected and used by third parties, and that they would be willing to change their behaviours and provide more extensive and accurate information to third parties if the consequences of doing so were made clearer. See: ICO (2015) "Data protection rights: what the public want and what the public want from Data Protection Authorities", available at: https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf and DataIQ (last accessed December 2017) "Consumers give firms false personal data due to a lack of trust", available at: http://www.dataiq.co.uk/news/201505/consumers-admit-lying-about-personal-data-due-lack-trust

of many scholarly conceptualisations of privacy, many of which were developed prior to the advent of digital technology.[8] A review of the literature in the field, for instance, reveals that various scholars throughout the twentieth century attempted to refine the notion of control in the context of privacy and data protection, and distinguish it from other competing interpretations of these two other concepts.

Perhaps most famously Alan Westin conceptualised privacy as control: the ability of the individual to dictate when, how, and to what extent information about them is communicated to other parties.[9] The notion of "privacy as control" therefore differs from other conceptualisations of privacy, such as considering privacy to be a "right to be let alone".[10] Despite this conception of privacy playing a prominent role in academic discourse for the best part of half a century, it has arguably become more salient in the present day than it has been at any other point in time and, as is considered in greater detail below, has recently been endorsed by European lawmakers and other observers as a means of responding to the types of regulatory challenges pertaining to the processing of personal data outlined above.

The crux of privacy as conceived in this way is the idea that the individual's self-determination and choices in respect of how their personal data are used should take precedence over other competing values and interests. In this sense, when envisaged this way, privacy can essentially be described as a form of information management, where control is achieved through the expression of an individual's preferences. The theory of privacy as control therefore, relies on the presumption that individuals are autonomous and rational beings, capable of determining for themselves whether and when they wish to disclose aspects of their personal data to others. Control, therefore, is conceptualised as an individual, dynamic, and flexible process which takes the shape of a right which entitles individuals to know which of their personal data are collected, to determine which of their personal data are made available to third parties, and to access and potentially make corrections in the event of any errors.[11]

Alongside the notions of self-management and individual choice of privacy as control some scholars have taken a different approach and conceptualised privacy as control in terms of property. A notable, and apparently growing, part of the privacy and data protection literature, for instance, considers whether greater individual control of personal data could be achieved through the leverage of market forces and making individuals "owners" of their data. According to such views, privacy can be likened to a property right. Though much of the academic scholarship in this vein has historically emanated from the USA,[12] it is now a topic which is drawing more attention from European scholars.[13] According to this view, the ability of the individual to control their personal data is directly related to the idea that they should be able to state legal or equitable ownership of them. As has been remarked elsewhere, in this sense the concept of control evokes ideas of absolute power or sovereignty over personal data which entail an "exclusivity axiom", which theoretically allows the owner of personal data to protect those

[8] Lazaro, C. and Le Metayer, D. (2015) "The control over personal data: True remedy or fairy tale?", script*ed* 12(1), pg.6.
[9] See, in particular, Westin, A. (1967) *Privacy and freedom*, New York: Atheneum Press.
[10] Fried, C. (1968) "Privacy", *Yale Law Journal*; Rachels, J. (1975) "Why privacy is important", *Philosophy & Public Affairs*; Schwartz, P. (2000) "Internet Privacy and the State", *Connecticut Law Review*; Cohen, J. (2000) "Examined Lives, Informational Privacy and the Subject as Object", *Stanford Law Review*; Solove, D (2013) "Privacy Self-Management and the Consent Paradox", *Harvard Law Review*.
[11] Lazaro, C. and Le Metayer, D. (n 8) pg.7. It should be noted that people have criticised the "privacy as control" conception of control, on the basis that "controlled" disclosures or uses of personal data can still lead to so-called "privacy harms", see: Allen, A. (2000) "Privacy-As-Data-Control: Conceptual, Practical, and Moral Limits of the Paradigm", *Connecticut Law Review* 32
[12] See Litman, J. (2000) "Information Privacy/Information Property", *Stanford Law Review* 52, pg.1286.; and Bergelson, V. (2003) "It's Personal but Is It Mine? Toward Property Rights in Personal Information", *U.C. Davis Law Review* 37, pg.383.
[13] See, for example: Purtova, N. (2014) "Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table…and back on again?", *Computer Law & Security Review* 30(1)

data from unwanted uses, sharing, and alteration, and grants them full alienable rights to those data, in a way that is similar to certain aspects of property law.[14]

What is particularly interesting about the competing conceptions of control as self-determination and control as property is that, despite the fact they appear to be anchored in entirely different legal and theoretical backgrounds, they share some similar assumptions about individual privacy. Both, for instance, appear to be inextricably linked to the idea that individuals are rational and autonomous agents who are both capable of forming personal preferences and goals, and determining courses of action by which those preferences and goals can be expressed and achieved. Both conceptions, therefore, appear to be grounded in individualism, a philosophical school of thought which emphasizes the moral worth of the individual at the expense of any competing interests of groups of individuals or the state.[15] Both conceptions, for instance, bestow upon the individual the ability to define, unilaterally and independently, their relationships with others, effectively rendering the crux of privacy as the ability of the individual to detach themselves from other individuals and society at large.

Additionally, according to this view, privacy also has an important active dimension as well as one which is strictly individualistic. This is particularly noticeable in respect of the way in which both conceptions of control are premised on individual agency and the ability of individuals to construct their lives in a way that they deem desirable.[16] Since, therefore, this active choice requires the individual to effectively participate in the management of their personal data, which may involve the voluntary alienation of data with regards to how those data are shared with others, control over personal data evidently cannot be reduced to a mere "right to be let alone".

However, despite various scholars and other observers' attempts to refine the notion of control, particularly through exploring its individualistic and active dimensions, it in many ways remains an imprecise and poorly understood concept. As has been noted elsewhere, for instance, defining control as a matter of information management without delving any deeper into its nature or meaning is to overlook important questions such as those relating to the extent of that control, or even what types of information an individual should be able to seek to control, or even what the fundamental underlying purpose of that control is.[17] To date, there appears to be a lack of academic literature that has convincingly explored many of these issues. Some, however, have commented on this lack of detailed examination, and suggested that if control is defined purely in terms of information management it can barely, if at all, be disentangled from other prominent theories of privacy, many of which all require or hinge upon, to some extent at least, a level of individual control.[18]

As a case in point, in 2008 prominent privacy scholar Daniel Solove articulated a taxonomy for six different types of privacy. Although one of Solove's six definitions was "privacy as control of one's personal information", the others mentioned were privacy as limited access to the self; privacy as the right to be let alone; privacy as secrecy; privacy as personhood; and privacy as intimacy.[19] However, it is not self-evidently clear how these other differing conceptions can be distinguished from the conception of privacy as control of personal information. It might be suggested, for instance, that ensuring that one is let alone, or that one's communications and dealings remain confidential, will necessarily require the individual involved to exercise at least a degree of control over certain types of information relating to them.

---

[14] Lazaro, C. and Le Metayer, D. (n 8)
[15] Wood, E. (1972) *Mind and Politics: An Approach to the Meaning of Liberal and Socialist Individualism*, Oakland, California: University of California Press, pg.6.
[16] Lazaro, C. and Le Metayer, D. (n 8) pg.8.
[17] Shoemaker, D. (2010) "Self-exposure and exposure of the self-informational privacy and the presentation of identity", *Ethics and Information Technology* 12(1), pg.4.
[18] Lazaro, C. and Le Metayer, D. (n 8). pg.9.
[19] See: Solove, D. (2008) *Understanding Privacy*, Cambridge, Massachusetts: Harvard University Press.

What can be concluded from this brief overview of the academic literature pertaining to privacy and data protection is that if control is conceived of as a concept within the rubric of information management it will necessarily be a key constituent part of most, if not all, conceptions of privacy, meaning the two concepts are apparently inextricably conflated. This conflation, however, is troubling as it blurs any possible theoretical distinction between the notion of control serving as a conceptual *foundation* for other concepts such as privacy and data protection, and the notion control serving as a tool for the *management* and *delivery* of other concepts like privacy and data protection – in other words, it hinders the answering of the question: precisely what theoretical justifications can be identified for putting individuals in a position of control of their personal data?

As a result, this conflation – along with a dearth of answers to other associated questions in respect of who it is who should exercise control, why they should exercise control, and what they should exercise control over – has arguably had the effect of diminishing any potential value control may have as a concept in and of itself.[20] In the immediate context this is perhaps particularly problematic for, as is discussed in the following section, the notion of individual control now has a pervasive presence throughout European data protection law and policy.

3. The notion of control of personal data in the European data protection framework

In recent years the suggestion that individuals should be afforded greater control over their personal has become a prominent notion in the rhetoric of EU institutions in the data protection policy arena. This is well-evidenced not only by speeches given by senior EU officials,[21] but also by the texts of an array of official policy documents and EU legislation, many of which couch the notion of individual control in terms that suggest it is a concept that is critical, if not a prerequisite, to individuals enjoying high levels of data protection.

This section of the article is dedicated to an analysis of several prominent documents and legislation in the EU data protection policy arena, and outlines their treatment of the notion of individual control. The documents considered here are of a diverse nature, and are not intended to be portrayed as an exhaustive list of all official EU policy documents in the data protection field but, instead, consist of a number of prominent and salient examples of such documents. They include: full legislative texts, preparatory texts for prospective legislation, expert opinions, and educational documents of a more casual nature aimed at EU citizens.

3.1 The General Data Protection Regulation and prior communications

The first, and perhaps most salient, document for our consideration is Regulation 2016/679, commonly known as the General Data Protection Regulation. As noted above, the Regulation will come into force in May 2018, and has been drafted as a means updating the European data protection framework in light of challenges posed by contemporary data-handling practices. This is well-evidenced early in the Regulation's text, where reference is made to a variety of regulatory issues caused by the development of digital technologies, and how many have come to undermine the effectiveness and enforceability of pre-existing data protection rules.

Particularly, Recitals 5 and 6 of the Regulation highlight the increased volume of cross-border flows of personal data, rapid technological developments, globalisation, the seemingly ever-increasing volume of the collection and sharing of personal data, and the lack of harmonisation of legal rules being

[20] Lazaro, C. and Le Metayer, D. (n 8) pg.9.

[21] For instance, in a 2011 speech, the Vice-President of the European Commission responsible for the EU's Digital Agenda project, Neelie Kroes, spoke at length about how enhancing individual control over personal data were vital for reinforcing trust and confidence in online services. See: European Commission Press Release Database (last accessed December 2017) "Online privacy – reinforcing trust and confidence", http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm

enforced by national data protection authorities as notable causes of these problems.[22] The upshot of this, the Regulation contends, is that there is now a need for a stronger, more coherent, regulatory framework which will ensure higher levels of data protection for EU citizens.

What is significant for the purposes of this article, however, is the way in which the notion of individual control of personal data appears to play a key role in respect of how the high levels of data protection the Regulation aspires to might be achieved. Notably, for instance, Recital 7 of the Regulation expressly states the importance of putting individuals in a position from which they can be said to "*have control of their own personal data*".[23] This is complemented and built upon by a number subsequent recitals.

Recital 68, for instance, specifies that in order to "*strengthen the control over his or her own data*" in matters pertaining to the automated processing of personal data, individuals should be allowed to receive copies of those data in a commonly used, machine-readable and interoperable format. Following this, Recital 75 states that one of the main forms of data processing activities involving personal data that might pose a threat to the rights and freedoms of individuals are those which may have the effect of preventing individuals from "*exercising control over their personal data".* Finally, Recital 85, addressing the issue of personal data breaches, states that "*A personal data breach may, if not addressed in any appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data…".*

From this, we can glean several things. Firstly, it can clearly be inferred that in the view of the Regulation establishing and strengthening individual control over their personal data is one way in which high levels of data protection can be achieved and, secondly, that a loss of individual control over personal data may actively impede an individual from enjoying high levels of data protection.

The text of the Regulation, therefore, can be said to embody the spirit and approach of an earlier communication adopted by the European Commission in 2012, entitled "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century",[24] a document which formed part of the foundation of the recent period of reform of the European data protection framework of which the Regulation is one of the end products. In the communication's introductory sections, for instance, it is explicitly stated that individuals should have the right to enjoy "*effective control*" of their personal data, with many of the subsequent sections of the document being dedicated to outlining the goal of "*putting individuals in control of their personal data*".[25] The communication then goes on to state that the main aim of the reform of EU data protection rules was "*to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively*".[26] This, it was suggested, would best be brought about by the introduction of new rules which will "*improve individuals' ability to control their data*".[27]

Interestingly, despite repeated mentions of the notion of individual control of personal data, neither the Regulation, nor the communication before it, include any definition nor elucidation of what is meant by control. The communication does, however, mention and highlight four precise objectives through which the enhancement of individual control could potentially be achieved. Broadly speaking, these precise objectives were all incorporated into the final text of the Regulation adopted by the European

[22] General Data Protection Regulation Recitals 5 & 6.
[23] *Ibid*., Recital 7.
[24] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committees of the Regions, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, Brussels, 25.01.2012.
[25] *Ibid*., pg.5.
[26] *Ibid*
[27] *Ibid*

Parliament in April 2016.[28] Foremost amongst the control enhancing objectives listed by the communication was the reinforcement of the doctrine of informed consent within the data protection framework.[29] Pursuant of this objective, the Regulation contains a new definition of consent which specifies that the processing of an individual's data can be legitimised by way of the individual indicating their freely given, specific, informed and unambiguous consent.[30] This attempt to strengthen, and to some extent reformulate, the data protection framework's rules regarding the doctrine of consent should in many ways come as no surprise for, as has been remarked elsewhere, from a fundamental rights perspective the doctrine of consent has traditionally been considered "*the best way for individuals to control data processing activities*".[31] At this point it is perhaps worth noting that when considered against the background of contemporary data handling practices this assertion now appears highly contentious, but nevertheless, practical concerns notwithstanding, the text of the Regulation strongly suggests European lawmakers consider consent to be capable of playing a key role in European data protection framework so far as establishing individual control over personal data is concerned.[32] However, perhaps recognising the limitations of the doctrine of consent, the Regulation goes further, and incorporates a number of other objectives articulated by the communication pertaining to the enhancement of individual control.

Perhaps the second most significant aspect of the Regulation which appears to have been born from the prior communication and is concerned with strengthening individual control of personal data is the introduction of the "Right to be forgotten". This new right is enshrined in Article 17 of the Regulation, and states that in certain situations individuals will have the right to obtain from another party holding their personal data the erasure of those data without undue delay.[33] It is further clarified in Article 17 that, amongst other situations, this right can be invoked in instances where the individual to whom those data relate withdraws their consent to those data being processed.[34] The practical effect of the right to be forgotten, therefore, could be to potentially force institutions and organisations handling an individual's personal data to comply with said individual's request to cease all processing activities associated with that individual's personal data, and potentially erase every piece of personal data they possessed in relation to that individual. In so doing, the right should in theory allow individuals to exert a degree of influence over their personal data, even once those data are no longer exclusively under the individual's personal jurisdiction.

The third of the communication's objectives pertaining to individual control that has been incorporated into the Regulation is the introduction of another new right, the right to data portability. This right is

---

[28] See: European Parliament (2016) "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era (last accessed December 2017)

[29] The consent of the individual data subject is currently one way in which the processing of personal data can be rendered legitimate under EU Data Protection Law. See: Data Protection Directive Article 7(a).

[30] Article 3(8) General Data Protection Regulation. See also, Article 6(1)(a)

[31] Committee on Civil Liberties, Justice and Home Affairs (2012) *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, (COM(2012)001 – C7-0025/2012 – 2012/0011(COD)), pg.200.

[32] On the limitations of consent as means of ensuring individual control of personal data in contemporary digital environments, see: Van Alsenoy, B. Kosta, E. and Dumortier, J. (2013) "Privacy notices versus informational self-determination: minding the gap", *International Review of Law, Computers and Technology;* Cate, F. and Mayer-Schonberger, V. (2013) "Notice and Consent in a world of Big Data", *International Data Privacy Law* 3(2).

[33] General Data Protection Article 17. The right to be forgotten is thought to be controversial for a variety of reasons, perhaps primarily because of its apparent potential for conflict with other legally enshrined values, such as freedom of expression. For a discussion of these issues, see: González, L. (2013) "Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression in online social networks", *Entertainment Law Review*

[34] General Data Protection Regulation, Article 17(b)

enshrined in Article 20 of the Regulation, and effectively provides that individuals will have the right to receive any personal data they have provided to another party in a structured, commonly used and machine-readable format, and have the right to transmit those data to another party without hindrance.[35] The crux of this provision appears to be that it will provide individuals with a novel legal right to transfer their personal data from one information service provider to another, effectively providing them with a means by which they can obtain an immediate and complete download of their personal data held by third parties, such as the providers of online services and mobile applications. In so doing, the right to data portability, not unlike the right to be forgotten, has been designed to allow individuals to exercise greater control over their personal data by allowing them to influence how those data are used by others, even after initially agreeing to share them with a third party.

The final key relevant objective of the communication in relation to enhancing individual control of personal data was to reinforce individuals' rights to information, and to guarantee data accessibility. These objectives have been incorporated in articles 13, 14 and 15 of the Regulation. Articles 13 and 14 respectively deal with situations in which personal data have, and have not been, collected from an individual. In effect they state that in either situation the controller of those data must provide the individual to whom those data relate with, within a reasonable period of time, amongst other things, the identity and contact details of the controller, the purposes for which the personal data in question have been collected, the categories of personal data concerned, where the personal data were acquired from, as well as the right of the individual to lodge a complaint with a supervisory authority.[36] Article 15 then builds on what is said by the previous two articles and states:

> "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed…*"[37]

Article 15 goes on to further state that, in the event that the individual receives confirmation that a third party has come into the possession of their personal data, the individual will have the right to access those data and any relevant information in relation to why the third party holds those data and for what purposes. Articles 13, 14 and 15 all also specify that one other piece of information that the individual must be provided with is that they have a right to object to any processing of their personal data to which they do not agree.

Despite this, at a glance at least, the provisions contained within Articles 13, 14 and 15 do not initially appear to be directly concerned with establishing individual control of personal data. They do not, for instance, contain any rights or mechanisms by which individuals can directly and actively attempt to assert control over their personal data. In this sense they can be said to differ from the other abovementioned provisions contained within the Regulation concerned with consent, the right to be forgotten and the right to data portability. They can, nevertheless, still be said to be directly relevant to the notion of individual control.

By focusing on ensuring the ability of individuals to be made aware of other parties who hold their personal data, and that the individuals concerned can access those data, we can see they instead appear to be concerned with establishing foundations for control that will surely be a prerequisite if the other previously initiatives explicitly concerned with individual control are to have any chance of practical success. If individuals do not have knowledge of the existence and whereabouts of their personal data, for instance, the practical efficacy of legal and regulatory initiatives which allow them to actively exert control over those data will surely be heavily undermined.

3.2 Works of the Article 29 Working Party

[35] General Data Protection Regulation Article 20.
[36] *Ibid*., Articles 13-14.
[37] *Ibid*., Article 15.

In addition to full legislative texts and associated prior communications, another form of EU policy document pertaining to data protection in which one can find numerous references to the concept of individual control of personal data are the works of the Article 29 Working party, a body made up of representatives from the data protection authorities of each EU member state and tasked with providing expert advice in matters pertaining to data protection law and policy.[38] Since its inception the Article 29 Working Party has produced a considerable number of advisory texts on the interpretation and application of various aspects of EU data protection law, many of which mention the notion of control.[39] For the sake of clarity and concision, however, this section of the article focuses on one relatively recent and salient example of such a text, the guidelines on the right to data portability adopted in December 2016.[40]

As highlighted above, the General Data Protection Regulation contains several provisions pertaining to individual control of personal data. In particular, Article 20 of the Regulation creates a new right to data portability, which allows individuals to receive their personal data from a third party who holds those data, and transfer those data to another party of the individual's choosing. The Working Party's guidelines on the new right, one of the first issues relating to the Regulation on which the Working Party has chosen to provide guidance, offers some insight into the potential interpretation and implementation of the new right, and provides some clarification in respect of the conditions under which the new right applies. Other than providing some interesting observations in relation to the interpretation of new right, however, what is particularly interesting about the guidelines is the treatment of the notion of individual control of personal data, and how it relates to the right. The notion of control is, for instance, expressly made reference to at a number of points. In particular, it is first suggested that the right to data portability has been designed to support:

> "…*user choice, user control, and consumer empowerment*."[41]

This is later complemented by the suggestion that the right also:

> "…*represents an opportunity to "re-balance" the relationship between data subjects and data controllers through the affirmation of individuals' personal rights and control over the personal data concerning them*."[42]

It is then further suggested that the ultimate objective of the right is:

> "…*to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject's control*".[43]

From this brief overview of the Working Party guidelines, we can glean a number of things. Firstly, the guidelines represent another example of an EU policy document pertaining to data protection which mentions, and appears to place key emphasis upon, the notion of individual control of personal data. In so doing, the guidelines appear to further reiterate the importance of individual control as a theme within the data protection policy area.

Secondly, the guidelines, as can be seen in the sections of the text quoted above, explicitly acknowledge that the right of data portability is primarily concerned with establishing, or at least enhancing, the

---

[38] Article 29 Working Party (Last accessed December 2017) http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[39] See, for example: Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 01197/11/EN WP187; Article 29 Data Protection Working Party, *The Future of Privacy*, Joint contribution to the Consultation of the European Commission on the legal framework of the fundament right to protection of personal data, 02356/09/EN WP168.

[40] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, 16/EN WP242

[41] *Ibid*., pg.3.

[42] *Ibid*., pg.4.

[43] *Ibid*., pg.5.

ability of individuals to control their personal data, and appears to envisage individual control as a solution to regulatory issues relating to existing observable imbalances which exist between individuals and other parties which may seek to obtain their personal data.

Pursuant of this, thirdly, and perhaps most interestingly, the guidelines recommend the use of technological tools and architectures as a means of implementing the right, seemingly acknowledging that individual control may require technological and structural assistance if it is ever to be meaningfully achieved. What is also significant, however, is the fact that despite mentioning control on a number of occasions, control itself is not a term that has been defined by the guidelines, nor is any comment provided as to its true meaning, scope or theoretical underpinnings.

3.3 Other

One final document that is also worth considering, albeit it briefly, is one issued by the European Commission in 2012 entitled "Take control of your personal data".[44] Unlike the other documents already considered, this publication takes the form of a short brochure and was seemingly designed to raise the awareness of EU citizens in respect of ongoing data protection reforms within the EU, and the significance of individuals routinely imparting with their personal data when engaging in online activities.

Of particular interest is the way in which the document expressly reiterates the objectives of the abovementioned European Commission communication, and states that the primary objective of the reform of the EU data protection framework was to "*put you in control of your own information"*.[45] Interestingly, this document being drastically different in nature from those already mentioned above, one obvious and significant similarity is the way in which it is structured, even to the extent to which the brochure alludes to technological architectures and tools that may be required in order for control of personal data to truly be established.

3.4 Discussion

From the above overview and consideration of a variety of policy documents published by EU institutions we can draw two important conclusions. Firstly, we can see that the notion of individual control of personal data is pervasively used and features heavily as a recurrent theme throughout EU data protection law and policy. This is well evidenced by its notable presence in a variety of different forms of policy documents, many of which appear to envisage the idea of individual control of personal data as both an important policy objective and, concurrently, as a means by which regulatory challenges associated with the use and collection of personal data, such as those outlined previously, can be counteracted.

Secondly, and perhaps more troublingly, we can see even though control has a pervasive presence in the data protection field at an EU level, the approach to control taken by the documents considered here in many ways appears even more muddled than the approach taken to control by the scholarly and academic literature considered above. As noted previously, according to the scholarly literature pertaining to control of personal data or information, the main dimension of the concept can be described as being almost entirely individualistic in nature. It appears, however, that whilst control as envisaged by EU data protection law also evidently has a notable individualistic dimension, it cannot be described in this way. Quite clearly the notion of control of personal data articulated by these documents envisage control as having considerable organisational and structural dimensions as well as those that are individualistic.[46] This can be inferred from all the documents considered above.

---

[44] European Commission (2012) *Take Control of Your Personal Data*. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

[45] *Ibid*

[46] Lazaro, C. and Le Metayer, D. (n 8) pg.13.

The General Data Protection Regulation, for instance, consists of several elements which could be said to embody the individualistic dimensions of control as articulated by the scholarly literature. A simple observation that can be made, for instance, is that that by granting individuals a variety of rights pertaining to consent, access, deletion and portability in respect of their personal data, the Regulation to some extent mirrors the main tenets of the theories of control touched upon earlier: the idea that individual empowerment germinates through individual choice and participative agency. In this sense, the mentions of the concept of control appear to allude to the individual's ability to make decisions about their personal data through active choice. The rights-based approach favoured by the Regulation, therefore, in theory, should equip the individual with the tools by which they can control the conditions under which their personal data are collected, processed, or shared by others. Similar observations can be made in respect how control is treated by the other EU policy documents also considered above.

Conversely, however, whilst the individual is clearly treated as a critical figure so far as the control of their personal data is concerned, the EU policy documents considered above clearly extend the notion of control beyond its purely individualistic dimension. Whilst initiatives such as rights pertaining to the deletion, access and portability of data obviously hinge on the involvement of the individual, they are evidently all initiatives which envision a notion of control that has considerable structural and operational dimensions. In other words, they are all initiatives that, for them to have any prospect of practical success, cannot be reduced to simply being matters of individual agency, autonomy and choice.

Irrespective of the wishes and desires of the individual, for instance, legal rights to access one's personal data, to have one's personal data deleted, or to have one's personal data moved from one third party to another, will be of little worth in contemporary digital environments if technological architectures which assist with their practical implementation are not established and put in place. This is most prominently acknowledged by the General Data Protection, which at numerous points alludes to this general sentiment.

As noted above, for example, Article 17, which as noted above outlines the right to be forgotten, refers to "*technical measures*" and "*available technology*" that data controllers should make use of when responding to an individual's data deletion requests. Similarly, Article 20, which enshrines the right to data portability, specifies that an individual will be entitled to obtain their personal data from one data controller and transmit it to another must be able to receive those data in a "*commonly used and machine-readable format*", the obvious implication being some degree technological support will be required if this right is to be effective in practice.

Further acknowledgement as to the structural and organisational dimensions of control can be found in Article 25, which considers the idea of data protection by design. Here it is specified that data controllers should, depending on the nature of their data processing activities and relevant costs, implement appropriate technological and organisational measures so to ensure a high degree of data protection for individuals. Reference here is also made to Article 42 of the Regulation which encourages the development and establishment of data protection and certification mechanisms and data protection seals and marks. In particular, it is stated that a certification mechanism as envisaged by Article 42 may be used as evidence to demonstrate compliance with Article 25's data protection by design requirements. As is also noted above, allusions to technical measures that may be required in order for control to be realised can similarly be found in the works of the Article 29 Working Party and other sources. All of these documents appear to indicate that EU regulators, whilst apparently committed to the idea of individual control of personal data, are aware of the fact that in contemporary digital environments control cannot merely be reduced to a matter of individual agency.

In any event, irrespective of the fact that the EU policy documents considered above apparently appeal to a notion of control that is not merely individualistic, thus rendering it an apparently more multifaceted vision of control than that which has been considered in the scholarly and academic literature, it can be

argued that the vision of control articulated by EU institutions is in any event at best far from comprehensive for a variety of additional reasons. In a worst-case scenario, it might even be argued that the concept of control as envisaged by the documents examined above is vague and detached from the key issues it apparently intends to address.

Primarily, for instance, by placing a heavy emphasis, and focusing almost exclusively, on the individual as a rational and autonomous agent, a figure who is presumed to have the capacity to make active and informed choices regarding their personal data, as well as the structural and organisational support that may be needed in order for them to do so, the documents obscure, or maybe even actively impede, the investigation of a number of significant unanswered questions as to the true nature of individual control in the data protection context.

Five notable questions that would apparently benefit from greater examination, but have apparently been paid scant attention by EU regulators, for instance, are: Precisely *who* is it that should be put in a position of control? Precisely *which* data should they should be put in control of? What should the *extent* of that control be? And, what underlying theoretical justifications can be identified for putting said individuals in this position of control? In other words, what is the rationale for putting people in control of their personal data? Is control in this context a means to protect another value such as privacy? Should control of personal data be thought of as a desirable and independent value in and of itself? Or is control in this context a notion that is linked to another rationale entirely? Finally, conceptual and theoretical difficulties aside, we must also surely ask *how*, in practical terms, the level of control desired by EU lawmakers can be achieved. As a means of further highlighting the inherent complexities of the notion of control's as envisaged in the EU data protection framework, these questions are considered in turn below.

3.4.1 Who should be put in a position of control?

The first of these questions regarding the notion of individual control relates to the identity of its agents. As outlined already, the EU policy documents considered above stress the importance of individual data subjects as rational and autonomous agents being put in a position of control of their personal data. However, a number of questions can be asked in relation to the appropriateness of this general position. Who, for instance, are these data subjects? Is it correct to assume they have the capacity to meaningfully participate in the administration of their personal data in the context of complex digital environments? Who in this context can ever truly be said to be in control? Troublingly, in relation to these questions, empirical research has suggested that the intricacy of contemporary digital environments is so elaborate and non-linear that to the average person they will likely be impossible to comprehend. It has also been shown that individuals frequently experience problems associated with self-control, prejudices, a lack of time, or apathy.[47] To this end, it appears that the existence several prevalent cognitive and behavioural challenges, all of which could conceivably curtail the individual's decision-making ability, may be extremely difficult to reconcile with the notion of control over personal data that is aspired to by EU lawmakers. Even if problems associated with cognitive biases and other related issues can be successfully overcome, however, this would not be the end of potential complications. As noted above, both the scholarly literature pertaining to individual control of personal data and EU policy documents pertaining to the control of personal data appear to consider control as a key solution to a number of regulatory challenges and potential harms linked to the usage and sharing of personal data in

[47] Such is the complexity of contemporary digital environments and online services and the like, many individuals often prefer to stick with default options rather than exercising features and functions that purport to allow them to control their personal data. See: Sunstein, C. (2014) "Active Choosing or Default Rules? The Policymaker's Dilemma", available at: https://dash.harvard.edu/bitstream/handle/1/12186290/activechoosingpaternalism5_14.pdf?sequence=1; Jensen, M. (2013) "Challenges of Privacy Protection in Big Data Analytics", *2013 IEEE Congress on Big Data*. Barocas, S. and Nissenbaum, H. "Big Data's End Run around Anonymity and Consent" in *Privacy, Big Data and the Public Good* (2014) ed. by Lane, J. et al. New York: Cambridge University Press. Pg.59

contemporary digital environments. As a corollary of this, one might infer that both the scholarly literature and EU policy documents imply that voluntary, or "controlled" uses or disclosures of information are not capable of causing any potential harms. There are, however, severe doubts to be had as to the standard of this logic.[48]

3.4.2 What should be the target of control?

The second question pertains to the subject matter of control, the concept of personal data itself. The EU policy documents considered above all stress the importance of allowing individuals to assume control over their personal data. However, the repeated emphasis of this general objective gives rise to ambiguities as to the scope of control. One might ask, for instance, whilst the policy documents considered above refer repeatedly to the importance of individuals being able to control their personal data, should this rhetoric be taken to encompass *all* of that individual's personal data? In other words, irrespective of whether it is practically achievable, does, or should, European data protection law aspire to give individuals the ability to control every single item of personal data relating to them? This is an issue which none of the policy documents considered above explicitly address, and so the answer is not especially clear.

If the answer to this question is no, then further questions can be asked in respect of precisely which personal data should be considered the legitimate target of individual control, and which should not. In other words, difficult questions would have to be asked in respect of how to design metrics through which different categories of personal data could be delineated as deserving of control or not deserving of control.

If the answer to this question is yes, however, then the subject matter of control as envisaged by EU policy documents would encompass a huge amount of information, much of which, as noted above, individuals may, even if they possessed the practical means to do so, may neither have the requisite time to control, nor have any interest in controlling. In this respect, it is important to remember that the scope of the concept of personal data as outlined above contains not only an individual's name, date of birth, and other biographical information, but also Internet Protocol addresses, browser histories, search engine results, location data, and other metadata.

In any event, questions can also be asked in respect of whether personal data should be the target of control at all. In this respect we might question what it really means to be in control of one's personal data in the context of contemporary socio-technical environments and data-handling practices, as well as what the true worth of controlling such data might be. Whilst the EU policy documents considered above do not expressly suggest that individual control might represent a panacea to emerging regulatory challenges pertaining to the collection and processing of personal data, we can clearly infer a belief on the part of EU lawmakers that control represents a promising way of providing some solutions to these issues. Given the prevalence of mentions of control across a range of different documents we might also conclude that not only is control considered a solution, but that it is considered a prominent and powerful solution.

However, as has been remarked elsewhere, individual control of personal data can immediately be dismissed as a complete solution to the plethora of regulatory issues related to phenomena such as "big data" and data mining and profiling activities, which in many instances may be capable of affecting individuals without any of their personal data initially being involved.[49] The construction of profiles by both public and private sector organisations, for instance, is thought to be a key driver of the regulatory challenges set out above. Significantly, however, these profiles are often constructed from data which

[48] Allen, A. (n 11)

[49] Ohm, P. (2009) "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review* 57.

do not fall within the definition of "personal data" as envisaged by the data protection framework.[50] In many cases it might be only after a profile of an individual has been constructed that it becomes "personal data". Accordingly, it has been suggested that for EU data protection policy to place as much emphasis on the control of personal data as it does is to fundamentally misunderstand the nature of some of the most significant regulatory challenges it currently faces, and that by focusing so heavily, on the concept of personal data, obscures the possibly negative effects of contemporary digital data-handling practices that do not necessarily involve an individual's personal data.[51] An individual having perfect control over their personal data would, for instance, do little to stymie harms originating from data processing activities not involving that individual's personal data. Conversely, even when such activities were to involve individuals' personal data, due to the ever-increasing sophistication of these types of practices the individuals whose data are involved will often not be aware, nor have any understanding, of their occurrence, who it is who is in possession of their personal data, and what the consequences of these activities might be. Either way, in both instances, the apparent value of the notion of individual control of personal data is strongly undermined.

3.4.3 What should be the extent of control?

The third question links closely to the second, but rather than being concerned with the subject matter of control, is concerned with the extent of control. As noted above, the EU policy documents considered previously stress the importance and value of individuals being put in control of their personal data, with the General Data Protection Regulation containing a range of substantive means by which it intends to achieve this objective. In so doing, the Regulation confers on the individual the sovereignty to make determinations in respect of how their personal data are used by others. In so doing, the Regulation appears to embody notions of individualism and autonomy.

As considered above, due to cognitive and behavioural challenges there are questions to be asked in respect of the appropriateness of this paradigm. Nevertheless, even if these challenges can be overcome, and we accept individuals should unquestionably be afforded control of their personal data, questions still need to be asked in respect of the extent of that control. For instance, we might ask if individuals are to enjoy sovereignty over their personal data, should that sovereignty be absolute? In other words, should an individual's preferences in respect of how their personal data are used and treated be unqualified?

In relation to these questions the Regulation appears to provide some guidance. Notably, Recital 4 of the Regulation makes it clear that an individual's data protection rights are not absolute, and must be balanced against competing societal interests. Additionally, the inclusion of a range of grounds for the legitimisation of personal data processing, several of which do not have any direct bearing to the wishes of the individual, appears to acknowledge the importance of other competing interests in the data protection framework. From this we can infer that evidently EU lawmakers do not in any way consider the individual's sovereignty in respect of their personal data to be incontestable.[52] Furthermore, many of the substantive provisions concerned with individual control contained within the contain qualifications and limitations as to their applicability, further illustrating this point. In particular, for instance, Article 17 of the Regulation which outlines the right to be forgotten specifies that the right

[50] Lazaro, C. and Le Metayer, D. (n 8) pg.22.
[51] Rouvroy, A. and Berns, T. (2013) 'Gouvernementalité algorithmique et perspectives d'émancipation': Le disparate comme condition d'individuation par la relation?" *Réseaux* 1(177) pg.179.
[52] The General Data Protection Regulation lists a number of grounds, other than the consent of the individual, upon which the processing of personal data can be rendered legitimate. These include, amongst others, situations in which the processing of personal data is necessary for the performance of a contract, when processing is necessary for compliance with a legal obligation, and when the processing is necessary for the legitimate interests of the data controller. See: Article 6 General Data Protection Regulation.

can only be invoked by an individual in a finite number of circumstances. Article 20 contains several similar provisions in respect of when the right to data portability can be invoked.

However, whilst from this we can infer that quite clearly the level of control over personal data European lawmakers believe an individual should be entitled to is *not* infinite, it is less easy to come to a definitive conclusion as to what the true extent of the sense of control they envision *is*. This is an issue which could potentially give rise to thorny practical issues, perhaps particularly in situations involving individuals who wish to exert control over information that is not only made up their own personal data but, simultaneously, the personal data of another individual.

To use a somewhat mundane example, difficulties may arise in situations where Person A is a contact of Person B. The fact that Person A and Person B are contacts is information which necessarily constitutes the personal data of both Person A and Person B. In this situation, if Person A wishes to divulge this fact to a third party, but Person B does not, then difficulties may arise in respect of whose control of personal data trumps that of the other.[53] Whilst this example may to many initially appear trivial, it demonstrates how, if the limits and scope of individual control of personal data are not clearly defined and understood, data protection rules designed to give individuals greater control of their personal data may potentially have the effect of reducing vertical power imbalances between individuals and third parties, such as online companies whose business models are built around the analysis of the personal data of their users, but may have the undesirable effect of creating other possible problems, such as horizontal power imbalances between individuals themselves.

3.4.4 What is the purpose of control?

The fourth of the questions posited above pertains to the theoretical aspects of control, and links closely to the considerations of control found in the academic and scholarly literature considered above. Whilst establishing individual control of personal data is plainly an important objective of the European data protection framework, and that control of personal data is evidently considered to be a means by which a number of emergent regulatory challenges can be overcome, it is not abundantly clear precisely whether control, as described and alluded to within the framework, is to be thought of as a *means* by which individuals can be afforded greater levels of privacy, data protection or autonomy in respect of their personal data and how they are used by others, or if control of personal data is to be considered a value in *itself* that is worthy of protection and, if so, why?

At a glance, this might initially seem a somewhat indulgent question. It is, however, a question that may have significant practical implications. The answer to this question, for instance, would help shed light on the answer to the other questions outlined and considered above and thus help to determine how the pragmatic elements of individual control of personal data might be fully realised.

3.4.5 How can control be achieved?

The final question pertains to the practical and pragmatic elements of control and, assuming the abovementioned conceptual and theoretical difficulties associated with the concept can be overcome, asks how, in practical terms, control over personal data in contemporary digital environments can be achieved. In this regard it is important to recall that the EU policy documents considered above, to a varying extent, all suggest how technological architectures and tools will likely be of considerable importance when it comes to establishing individual control over personal data.

However, these references to technological architectures and tools do not contain any substantive guidance on precisely which, or what kinds, of these types of services might be particularly useful in this regard, and so might be described as being somewhat vague. Separately from EU policy documents various suggestions have been put forth as to precisely which types of technological tools might be of

[53] Grimmelmann, J. (2009) "Saving Facebook", *Iowa Law Review*, 94, pg.1194.

assistance, with personal data stores and blockchain technology representing two prominent examples, but there are numerous questions still to be asked in respect of the extent to which they may prove useful in this context.[54]

Questions as to the practical dimensions of control are not, however, necessarily restricted to questions of technology. It might be, after all, that additional legal rules and regulatory frameworks will be needed if individual control over personal data is ever to be truly realised, irrespective of whether such control is technologically assisted or otherwise. It has been suggested elsewhere, for instance, that if control necessarily requires assistance from technological tools and architectures, a potential concern is the fact that at present there appears to be no bespoke regulatory framework pertaining to the use of such technologies. The absence of such a regulatory regime could possibly lead to problems in respect of matters such as the security and interoperability of such tools, as well as issues in relation to fair competition.[55] Others have gone further and suggested that if individual control over personal data is ever to be truly realised individuals themselves may have to be granted additional legal rights, outside the remit of data protection law, that they can assert in relation to those data. In this regard, as touched upon above, there appears to be a growing body of work advocating the introduction of property rights in personal data, with some going so far as suggesting that the introduction of the right to be forgotten, considered above, represents the first step towards the formal recognition of such rights within the European legal order.[56] Evidently, these are all issues and questions that will need to be engaged with if the practical elements of individual control are to be established.

By briefly considering these five questions in turn it is evident that there is both the potential and the need to further discuss and examine the notion of individual control as contained within the European data protection framework so that we can arrive at a more nuanced understanding of its philosophical and theoretical nature, to say nothing of its practical elements. One potentially promising avenue of enquiry which may help us develop our understanding of control as a part of data protection law is to examine another area of law that is also concerned with establishing individual control over certain types of information and things that are personally linked the individual, namely: the doctrine of moral rights, an important aspect of intellectual property law.

4. Moral Rights

Intellectual property law as a distinct field of legal practice regulates the creation, use, and exploitation of mental or creative labour. It creates proprietary interests in a diverse range of things, including novels,

---

[54] See, for example: Wright, A. and De Filippi, P. (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664; Van Kleek, M. and O'Hara, K. "The future of social is personal: the potential of the personal data store" in *Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society*, ed. by Miorandi, D. et al. (2014) Berlin: Springer-Verlag, pp125-158; Pearce, H. (2015) "Online data transactions, consent, and big data: technological solutions to technological problems?", *Computer and Telecommunications Law Review* 21(6).

[55] See: De Filippi, P. (2016) "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production*. Available at: http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-; Glass, P. (2016) "How secure is blockchain?", *Taylor Wessing*. Available at: https://united-kingdom.taylorwessing.com/download/article-how-secure-is-block-chain.html; [55] McLean, S. and Deane-Johns, S. (2016) "Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?", *Morrison Foerster*. Available at: https://media2.mofo.com/documents/160405blockchain.pdf; Greenwood, D. et al. "The New Deal on Data: A Framework for Institutional Controls" in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. by Lane, J. et al. (2014) New York: Cambridge University Press. pg.203; Sweatt, B. (2014) "A new model for data sharing", *Significance* 11(4).

[56] See: Purtova, N. (2014) "Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table…and back on again?", *Computer Law & Security Review* 30(1); Ausloos, J. (2012) "The 'Right to be Forgotten' – Worth Remembering?", *Computer Law & Security Review* 28(2).

computer programs, paintings, films, television broadcasts and live performances, and through copyrights, patents and trademarks affords the authors or creators of such works a range of economic and pecuniary rights.[57] Alongside these core aspects, another key component of the majority of contemporary intellectual property regimes is the doctrine of moral rights. These rights, are entirely separate from an artist's pecuniary or economic interests and have evolved to protect the creative efforts of artists in their works.[58]

Derived from the French *droit moral*, in this context the use of the word "moral" is not intended to be interpreted as meaning the opposite of immoral or amoral. Instead, the term is intended to convey an element of ethics or societal interest.[59] Today these rights are well-established in a number of legal systems throughout Europe, perhaps reflecting the high value European culture places on artistic expression. In particular, the key essence of the doctrine of moral rights can be described as including:

> "*...non-property attributes of an intellectual and moral character which give legal expression to the intimate bond which exists between a literary or artistic work and its author's personality; it is intended to protect his personality as well as his work.*"[60]

Under the moral rights doctrine, the author or creator of a copyrightable work is, generally speaking, able to exercise control over that work in a number of notable ways, though some divergence exists between the extent and scope of moral rights between different states.[61] Most European nations are, however, members of the Berne Convention,[62] an international agreement governing the use of copyright which, since its revision by the Rome Copyright Convention in 1928, has provided standards for the protection of moral rights. At the 1928 Berne Conference in Rome, the Italian delegation drafted the most comprehensive proposal for inclusion of moral rights in the Convention, and described these rights as follows:

> "*...it is agreed today that, independently of the exclusive rights of economic character, which are essentially temporary and transferable, the author does own one right, or a set of rights, strictly inherent in his person, that are intransferable and without limitation in time, and which mainly concern the absolute right to publish or not to publish the work, to recognition of authorship and finally to the protection of the integrity of the work."*[63]

Pursuant of this, the Convention describes two main rights to which the creators or authors of artistic works should be entitled: the right of attribution, sometimes also referred to as the right of paternity, which broadly speaking can be described as the right of the author or creator to be named when their work is copied or communicated to others, and the right of integrity, which broadly speaking can be described as the right to control the form of that work. Both of these rights are examined in greater

---

[57] Bently, L. and Sherman, B. (2009) *Intellectual Property Law*, Oxford: Oxford University Press pg.1.
[58] *Ibid*., pg.241.
[59] Leimer, S. (1998) "Understanding Artists' Moral Rights: A Primer", *Public Interest Law Journal*, pg.42.
[60] Sarrute, R. (1969) "Current Theory on the Moral Right of Authors and Artists under French Law", *The American Journal of Comparative Law* 16(4), pp.465-486.
[61] The moral rights recognised in the United Kingdom under the Copyright, Designs and Patents Act 1988, for instance, are thought to be more limited that the rights granted in various other jurisdictions. In this respect, it is worth noting that the European Union, despite the fact that it has harmonised virtually every aspect of copyright protection, has excluded moral rights from its harmonisation efforts on numerous occasions. See, for example: Directive 2001/29 EEC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society.
[62] Formally known as the Berne Convention for the Protection of Literary and Artistic Works. Hereinafter the Convention.
[63] Quoted in Wilkinson. M. and Gerolami, N. (2004) "The Information Context of Moral Rights under the Copyright Regime", *Law Publications*, available at: http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1077&context=lawpub

detail below, but for now it sufficient to focus specifically on the first paragraph of Article 6*bis* of the Convention, which states that:

> "*Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work, and object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honour or reputation."*[64]

By looking at Article 6*bis*, we can see that moral rights, as envisaged by the Berne Convention at least – by allowing individuals to assert authorship in respect of artistic works, and deny undesirable future treatment of those works – appear to primarily be concerned with establishing and giving effect to individual autonomy and control. They aim to grant the creator of an artistic work the sovereignty to assert a connection to their work, and potentially to determine how that work is used and treated by others.

However, whilst moral rights appear to be prima facie concerned with the notion of individual control, it might be argued that they do not represent an obvious point of reference or comparison for investigating the notion of control as contained within data protection law, an entirely distinct field of legal practice. As noted above, for instance, intellectual property law is concerned primarily with establishing control over intangible assets like inventions, designs and other artistic works. Conversely, data protection law is primarily concerned with establishing rules regarding the use of personal data which, as also noted above, is defined as information that can be related to an identifiable individual.

Whilst personal data and the subject matter of intellectual property law may share similarities in that personal data, like copyrights and other aspects of intellectual property, are intangible, it can be argued that they are qualitatively different. Personal data are, for instance, information that will often be generated by an individual as a result of their very existence. The individual to whom those data relate enjoys the protection of those data as a fundamental right.[65] Conversely, the same individual can only come to hold intellectual property rights, be they moral rights or another form of intellectual property rights, because of some artistic endeavour. Accordingly, it might be suggested that data protection rights and moral rights have qualitatively different theoretical roots and rationales, and thus, are ill-suited for comparison with one another. As will be argued below, however, due to a number of apparent theoretical and practical similarities between the two fields, it appears there may be considerable potential for one to help develop our understanding of the other.

At this point it is perhaps important to note that in the literature there exists a degree of opposition to the notion of moral rights, some which attacks the very theoretical foundations of the doctrine.[66] This article neither necessarily supports nor contends such lines of argument. Whilst discussions as to the validity of the foundations of moral rights are no doubt important for intellectual property scholarship, a detailed consideration of these matters is beyond this article's scope, and will only be touched upon to the extent necessary to engage with the article's overarching aims. In this respect, as one of the primary aims of this article is to examine the key constituent aspects of the doctrine of moral rights to see whether their consideration may help us develop an improved understanding of the concept of individual control envisaged by European data protection law, the theoretical foundations of moral rights, the legitimacy of which notwithstanding, are a logical starting place for this investigation.

4.1 The theoretical foundations of moral rights

At the root of the doctrine of moral rights there are two basic assumptions. First, the doctrine assumes that an artistic work can, or even should, be considered an extension of the creator of that work

[64] The Berne Convention Article 6*bis*.
[65] See: Charter of Fundamental Rights of the European Union, Article 8.
[66] See: Adler, A. (2009) "Against Moral Rights", *California Law Review* 97(1)

themselves. As alluded to above, the work of the creator according to moral rights is an "*expression of their innermost being*",[67] and that moral rights themselves "*spring from a belief that an artist in the process of creation injects his spirit into the work*".[68] From this starting point some observers have gone as far to suggest that the works of an author or creator should, under the moral rights doctrine, be thought of as extensions of the author or creator's personhood. Merryman and Elsen, for instance, suggest that to mistreat an artist's work is to "*mistreat the artist*".[69] In a similar vein, it has been suggested elsewhere that the existence of the doctrine is linked closely to ideas of individual autonomy and self-determination.[70]

The second assumption, which is closely related to the first, is that the works of an author or creator are deserving of special legal treatment, or indeed protection, because they and their integrity are, in and of themselves, extremely valuable. As was stated in a notable French case, moral rights "*protect the superior interests of human genius*".[71] Here it was suggested that the works of authors and creators must be preserved as the authors and creators themselves originally intended, as doing so would allow for their genius to be "*conveyed to posterity without damage*".[72] Accordingly, moral rights protect not only the individual interests of the author or creator, but also the interests of the wider public inasmuch as they preserve for posterity the object that represents the author or creator's supposed genius, or at least their uniqueness. This spirit is effectively summarised by Merryman, who notes:

> "*[T]here is more at stake than the concern of the artist…There is also the interest of others in seeing, or preserving the opportunity to see, the work as the artist intended it, undistorted…We yearn for the authentic, contact with the work in its true version.*"[73]

In this vein, various pieces of legislation pertaining to the protection of moral rights worldwide have been justified by way of reference to how such laws serve the public interest through preserving cultural heritage and ensuring the accuracy and integrity of an artist's works.[74] This sentiment is encapsulated by Wilkinson and Gerolami, who suggest that moral rights protect:

> "*…the public's right to be assured that a work represented to emanate from that author is in fact as the author constructed it…"*[75]

To this end, it can be argued that in the ever developing "information society", where sources of information and channels of distribution are rapidly increasing, the authority of information, as well as the reliability and currency of information, are of critical importance. To this end, it would appear, as a result, that the need for the social and economic role played by moral rights is increasing. The moral rights doctrine is, for instance, one way in which we can ensure that information can be associated with its source.[76] The outcome of ensuring this accuracy should be to assist the public in identifiable relevant

---

[67] Merryman, J. and Elsen, A. (2007) *Law, Ethics and the Visual Arts*, Kluwer Law International, at 423.
[68] Adler, A. (n 66) pg.3.
[69] Merryman, J. and Elsen, A. (n 67)
[70] Netanel, N. (1993) "Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation", *Rutgers Law Journal* 24; Spence, M. "Justifying Copyright" in *Dear Images: Art, Copyright and Culture*, ed. by McClean, D. and Schubert, K. (2002) London: Ridinghouse.
[71] *Tribunal civil de la Seine*, May 20 1911, Amm. I 271, quoted in Merryman, J. (1976) "The Refrigerator of Bernard Buffet", *Hastings Law Journal*.
[72] *Ibid*
[73] Merryman, J. (n 71)
[74] See, for example: The Visual Artists Rights Act 1990 (VARA) of the United States of America.
[75] Wilkinson, M. and Gerolami, N. (n 63)
[76] *Ibid*

and reliable information for their needs, which in turn will help progress economic and scientific endeavours and provide other benefits to wider society.[77]

Accordingly, from this overview we can identify that the doctrine of moral rights has both individualist and seemingly collectivist dimensions inasmuch as its underlying rationale appears to be to provide benefits for both individuals, in that moral rights are geared towards the protection of their personhood, or at least an extension of that personhood, and to wider society in that they aim to ensure the preserve the integrity and veracity of information. Significantly, what is particularly interesting about this overview in the context of this article is that both the individualistic and collective theoretical justifications for the doctrine of moral rights appear to bear a strong correlation to those which are often offered in relation to the justification of the existence of data protection law.

For instance, it is clear that the doctrine of moral rights relies on a nexus between an author and their creations, and aspires to protect the personal and reputational value of creative works rather than any monetary or financial value those works might have. Whilst this basic premise has been criticised due to it being based on an outmoded and romanticised image of authors and creators of artistic works that bears little relation to reality, there is little doubt that the crux of the doctrine is the notion that creators share an "*indestructible creational bond*" with their intellectual works.[78]

At this point it is important to recall that, as noted above, the artistic works of an individual and the personal data of an individual are qualitatively different concepts. Though the concept of personal data enjoys a broad definition, personal data categorically do not constitute intellectual works, nor are they, strictly speaking, "created" by the individual through any form of creative process. Accordingly, it holds to reason that there can be no "creational bond" between an individual and their personal data.

Nevertheless, because of the nature of personal data, it can still be suggested that there exists an inextricable link between those data and the individual to whom they relate. For instance, the existence of data protection law has been justified on the basis that an individual's personal data can be considered the manifestation of that individual's personality, and that accordingly, one of the primary functions of data protection law, by setting rules regarding the uses of personal data, is to provide protections to the self just as property law and intellectual property law protect material or intellectual goods respectively.[79]

Just as the moral rights scholarship suggests that to mistreat the work is to mistreat the artist, a survey of the scholarship on privacy and data protection reveals a similar attitude regarding the mistreatment of personal data. Stevenson, for instance, suggests:

> "*…we must learn to think of personal data as an extension of the self and treat it with the same respect we would a living individual. To do otherwise runs the risk of undermining the privacy that makes self-determination possible.*"[80]

---

[77] *Ibid*., For a detailed analysis as to the public interest in the existence of moral rights see: Wilkinson, M. (2006) "The Public Interest in Moral Rights", *Michigan State Law Review* 193. See also: Ong, B. (2002) "Why Moral Rights Matter: Recognizing the Intrinsic Value of Integrity Rights", *Columbia Journal of Law & The Arts*, pp.297-312.

[78] Dietz, A (1994) "The Artist's Right of Integrity under Copyright Law – A Comparative approach", *International Review of Industrial Property and Copyright Law* 177.

[79] Vitale, M. (2011) "Control Over Personal Data, Privacy and Administrative Discretion in Europe and The USA: The Paradox of Italian "Data Protection Authority", *The John Marshall Journal of Information Technology & Privacy Law* 30(4).

[80] Quoted in *Ethical Technology Use, Policy and Reactions in Educational Settings*, ed. by Beycioglu, K. (2012) Hershey, PA: IGI Global. Pg.87.

A similar sentiment was discussed in a 2016 Microsoft Research talk by the famous American computer scientist Butler Lampson which focused on the individual control on personal data,[81] and has also come to be considered in general discourse and the media.[82] This assertion is perhaps made more convincing by empirical research which has demonstrated that certain types of personal data, particularly when cross-analysed with each other, are capable of be deeply revealing as to an individual's identity.[83] Accordingly, there appears to be an immediately obvious underlying similarity between constituent aspects of the rationales for moral rights and data protection rights. Both appear to be prima facie concerned with providing the individual with protection in respect of something that is directly and inextricably linked to their personality. In other words, both aim to protect something that is "personal" to the individual.

The way in which the existence of moral rights and data protection rights can be justified by way of reference to a need to protect aspects of an individual's personhood is not, however, the only similarity that can be observed regarding the theoretical underpinnings of these two different areas of law. Further similarities between the two can also be identified in conjunction with their collective aims as well as those which might be described as individualistic.

As noted above, whilst the doctrine of moral rights is perhaps primarily concerned with providing individuals with a means by which they can exert control and influence over artistic work which they have created, another of its underlying purposes is to guarantee the accuracy of information which, in turn, is intended to provide wider societal benefits. This, again, appears to strongly correlate with another of the underlying justifications for the existence of data protection law and its associated rights.

As has been noted extensively elsewhere, for instance, the data European data protection framework has twin objectives. The first, as explained above, is to establish rules and provide individuals with rights in respect of the protection of their personal data. The second is to facilitate the free flow of data in the EU's internal market.[84] This can clearly be inferred from the recitals of both the Data Protection Directive and the General Data Protection Regulation, which suggest that an absence of harmonised rules regarding the protection of personal data might seriously adversely affect the establishment and functioning of the common market.[85] As also touched upon above, the Regulation also expressly states how the processing of personal data should be designed to serve mankind, and whilst data protection law confers specific rights upon individuals, these rights must be considered in relation to their function and impact on wider society and, if necessary, balanced against other competing interests in accordance with the principle of proportionality.[86]

---

[81] Microsoft (last accessed December 2017) "Personal Control of Data", https://www.microsoft.com/en-us/research/video/personal-control-of-data/

[82] The Guardian (last accessed December 2017) "Beware the rise of the digital oligarchy", https://www.theguardian.com/media-network/2015/mar/05/digital-oligarchy-algorithms-personal-data

[83] For instance, a 2013 study by the National Academy of Sciences of the United States of America demonstrated that a wide variety of an individual's personal attributes, ranging from their sexual orientation to intelligence, can be automatically inferred from personal data taken from social networking sites such as Facebook. Kosinski, M. Stillwell, D. and Graepel, T. (2013) "Private traits and attributes are predictable from digital records of human behaviour", *Proceedings of the National Academy of Sciences of the United States of America*. pg.4.

[84] See, for example: Beling, C. (1983) "Transborder Data Flows: International Privacy Protection and the Free Flow of Information", *Boston College International and Comparative Law Review* 6(2); Schwartz, P (1994) "European Data Protection Law and Restriction on International Data Flows", *IOWA Law Review* 471; Kong, J. (2010) "Data Protection and Transborder Data Flow in the European and Global Context", *European Journal of International Law* 21(2); Brownsword, R. and Goodwin, M. (2012) Law and the Technologies of the Twenty-First Century, Cambridge: Cambridge University Press, pg.308.

[85] See: Data Protection Directive Recital 3; General Data Protection Regulation Recitals 3-11.

[86] General Data Protection Regulation Recital 4.

An endorsement of this general notion can also be found in the case law of the CJEU and in other EU policy documents. In the *Lindqvist* case, for instance, the CJEU remarked that one of the primary aims of establishing Europe-wide data protection rules was to substantially increase cross-border data flows, which in turn would lead to increased levels of societal activity and development.[87] More recently, this idea has been reaffirmed and expanded upon by a variety of other documents published by the European Commission concerned with establishing a regulatory frameworks geared towards the maximisation of economic uses of data.[88] Clearly, therefore, one of the primary rationales behind the deployment of data protection law within Europe is a desire to provide wider societal benefits through the setting of rules regarding the use of personal data, as well as benefits that are enjoyed exclusively by individuals.

Having examined some of the theoretical foundations of both the doctrine of moral rights and of European data protection law, we can see that there are various observable similarities between the two. Even though on the face of things they appear to be entirely distinct areas of legal scholarship and practice, the existence of both can be justified by way of reference to the extremely similar individualistic and societal benefits they purport to provide. Both, moral rights and data protection rights, are premised on the notion that individuals should be afforded legal rights in relation to the uses of certain types of information or objects that are somehow personal to them when doing so is necessary to protect fundamental aspects of their identity. Both are concerned with objects or types of information that are, on some level at least, intrinsically linked to an individual's inner-self.

In addition to, and alongside, these individualistic justifications, however, both moral rights and data protection rights are also frequently justified on the basis that granting individuals rights in respect of objects or information with which they have an inexorable link will also prove hugely beneficial to wider society, particularly through ensuring the accuracy and integrity of information, which in turn will assist with economic and social development. Whilst there may be debates to be had as to the cogency of these lines of argument, it seems clear that the existence of both doctrines is rooted in similar theoretical ground. If, however, we are to delve deeper, and examine the practical dimensions of the doctrine of moral rights in addition to the purely theoretical, it is possible to discern further similarities. To demonstrate this assertion, by using the law of the United Kingdom as a case study, what follows is an examination of how two staples of the doctrine of moral rights, the right of attribution and the right of integrity, have been implemented in practice.

4.2 The right of attribution

The right of attribution, which as noted above is sometimes referred to as the right of paternity, gives the creator of a work to have their name accurately associated with their work. In other words, where the laws of a country recognise the right of attribution, the creator of a work may insist that their name appear on the work itself. If their name is not displayed the artist will have a valid cause of action in court. Conversely, the right of attribution may also be used to prevent another individual falsely attributing their name to a work of the work's creator. The right of attribution, therefore, helps to maintain and protect the relationship between a work and its creator.[89]

In the United Kingdom the right of attribution is governed by sections 77 to 79 of the Copyright, Designs and Patents Act 1988.[90] Here, it is specified that in order for the right to arise it is necessary to show two things. First, it is necessary to show that the work over which the creator attempts to assert the right a type of work to which to the right applies.[91] Significantly in this regard, the right of attribution under

[87] Case C-101/01 *Bodil Lindqvist*
[88] See, for example: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Building a European Data Economy*, COM(2017) 9 final, Brussels, 10.1.2017
[89] Leimer, S. (n 59) pg.47.
[90] [Hereinafter CDPA 1988]
[91] S.77 CDPA 1988

the CPDA only applies in relation to a limited number of works, specifically: original literary, dramatic, musical and artistic works, and films. Concurrently, the CPDA also makes clear that the right does not apply to computer programs, typefaces, or other computer-generated works. Second, it is also necessary for the creator of a work to have asserted their right of attribution.[92] A creator's right of attribution is not automatic and will not be taken to arise until it has been asserted.

So long as these two criteria are satisfied, the creator of a work will enjoy the right to attribution, and the right will be considered to have been infringed if one of two conditions have been met. Either a situation must arise in which the creator is either not properly identified as the creator of their work, or a situation must arise in which the work is dealt with in circumstances where attribution is required. In relation to the first condition, to be properly identified the name of the creator of a work must appear either in or on every copy of that work in a clear and competent manner, and in a way that is likely to bring their name to attention of anyone who comes into contact with that work.[93] In relation to the second condition, attribution will be deemed to be required in a variety of different situations, depending of the nature of the work in question.

In the context of literary or dramatic works, the creator has the right to be identified whenever copies of their work are published commercially or otherwise broadcast to the public.[94] Creators of musical works will be entitled to a right to be identified when such a work is commercially published, but the right does not extend to situations in which the work is either publically performed or broadcast.[95] Creators of artistic works have the right to be identified where their works are published commercially or exhibited in public, creators of architectural works have the right to be identified in relations to buildings that have created, and creators of filmed works have the right to be identified whenever such a work is publicly shown.[96]

The right to be named as the creator of a work carries with it a number of symbolic, economic and cultural consequences. Being named as the creator of a work, for instance, allows for the facilitation of intellectual works (for instance, through indexes, catalogues and bibliographies), the channelling of royalties (for example from the public lending right), the interpretation of the work (insofar as it provides a psychological or bibliographical history), the celebration, reward or sustenance of authorial talent or genius, and the construction of the individual as the creator of an intellectual oeuvre.[97]

From this overview of the right to attribution as envisaged by the law of the United Kingdom we can see that, broadly speaking, the crux and practical effect of the right is that it allows a creator of certain types of creative works to assert their identity as the creator of those works when said works are subject to certain types of treatment by others. One possible comparison that we can immediately perhaps make between the practical aspects of the doctrine of moral rights and data protection rights is the way in which the right of attribution under the CPDA bears some similarities to the right to information and the right to access personal data contained within the General Data Protection Regulation outlined above.

As considered previously, the effect of Articles 13 and 14 of the Regulation is that they, broadly speaking, provide the individual with the right to be provided with certain types of information when personal data about them are collected. In particular, it is specified that the individual is entitled to be made aware of when, why, where and what kinds of personal data are collected from them, or from other sources, and who it is who is responsible for these collections and subsequent uses. Once the

[92] *Ibid*
[93] S.77(7)(a) CDPA 1988
[94] *Ibid*
[95] S.77(2) & S.77(3)
[96] S.77(4) CPDA 1988
[97] Bently, L. and Sherman, B. (n 57) pg.244.

individual has been made aware of this information, this should then form the basis for them to exercise a range of other data protection rights linked to individual control.

Both the right of attribution as envisaged by the CDPA and the rights of information and access contained within the Regulation, therefore, appear to be primarily concerned with allowing the individual to assert their connection in relation to something that is personal to them and intrinsically linked to their identity, particularly in situations where that personal thing is subject to certain types of treatment by others. To this extent, both can be said to be concerned with establishing individual control, or at least establishing the foundations thereof.

As noted above, the right to be named as the creator of a work under the right of attribution carries with it a number of symbolic, cultural and economic consequences. Interestingly, the right of access to personal data, which indirectly allows individual to assert a connection between themselves and their personal data might also be said to carry with it similar consequences. As considered previously, in the present day an individual's personal data can, for instance, be used to make wide-ranging determinations in respect of their identities. This can range from determinations that are made in respect of their religious and political affiliations and sexuality, to determinations in respect of their credit-worthiness and other financial issues.[98] By providing individuals with a means by which they can assert their connection to their personal data, the right of access allows them to influence the facilitation and interpretation of their personal data by ensuring that other parties handling those data are aware that the data are definitively linked to the individual in question, which should in theory increase the probability of any determinations being made in respect of those data being accurate. Furthermore, the objective of asserting this connection between the individual and a thing that is personal to them, under both the CDPA and the Regulation, appears to be premised on the notion that by allowing the individual to make this assertion will either allow them to form a platform from which they can exercise other legal rights, or pursue other preventative measures, both of which will allow them to safeguard against possibly undesirable conclusions being made in respect of some aspect of their identity, or possibly some other negative consequence(s). To reiterate, in essence, both are concerned with allowing the individual to assert some form of control over something that is personal to them by way of allowing them to state their connection to it.

4.3 The right of integrity

Whilst some similarities can be observed between the right to attribution and certain data protection rights, it would appear that there are additional, possibly more pronounced, similarities between data protection rights and another staple of the doctrine of moral rights, the right of integrity. The right of integrity, unlike the right of attribution, protects the integrity of a creator's work itself, rather than the relationship between the creator and the work. Essentially, it is a right which prevents anyone from modifying a work without the creator of that work having first authorised such a modification. As with other moral rights, the creator of a work will retain their right of integrity even after transferring the legal ownership of the work, and possibly the copyright in that work, to another person. Therefore, the new owner of the work, even if they are the copyright holder of that work, must seek the consent of the creator before making any changes to it. In so doing the creator of the work retains sovereignty to control their creative expressions as well as the creative process associated with those expressions.[99]

As with the right of attribution, in the United Kingdom the right of integrity is governed by the CDPA and is given to the creator of literary, dramatic, musical, filmed and artistic works. In order for the right to be infringed, the creator of such a work must be able to demonstrate that there has firstly been a "derogatory treatment" of the work; that the work has been dealt with in circumstances where the author

[98] See: Houses of Parliament: Parliamentary Office of Science & Technology (2014) "Social Media and Big Data", *POST note 460*.
[99] Leimer, S. (n 58) pg.50.

is protected from derogatory treatment; that no exceptions apply; and that there has been no waiver by the creator as to their integrity right. Treatment in this context has been taken to mean any addition to, deletion from, alteration to or adaptation of the work, and it would appear that in order for a "treatment" of a work to occur the internal structure of the work must be interfered with.[100] Section 80(2)(b) of the CPDA then specifies that a treatment will be considered derogatory if it amounts to a "mutilation" or "distortion" of the work, or if it is otherwise prejudicial to the honour or reputation of the author.[101]

The right of a creator to object to, or prevent, the derogatory treatment of their work only arises where the work or copies thereof are dealt with in certain ways.[102] While these acts vary according to the category of work involved, they essentially arise where someone communicates, disseminates, or otherwise renders the derogatory treatment available to the public. As a result of this requirement, the right to integrity as envisaged by the CDPA is not a right which can be invoked in order to prevent the destruction or spoliation of the work itself.[103]

To summarise, the right to integrity, therefore, allows creators to exert control over their works by providing them with a legal mechanism by which they can object to any deletion, alteration, or adaptation to their work which is both prejudicial to their honour, and communicated to the public at large. Once again, in this sense, we can draw similarities between the right to integrity and a number of provisions pertaining to individual control in the General Data Protection Regulation. As noted above, whilst the works of a creator and the personal data of an individual are qualitatively different, they are both intrinsically linked to the individual in the sense that they represent something personal to that individual.

Accordingly, like the right of integrity, the Regulation provides individuals with a number of means by which they can object to the treatment of something that is personal to them and demand a cessation of that treatment. In particular, as noted above, the rights to information and access in relation to an individual's personal data enshrined in Articles 13, 14 and 15 of the Regulation all mention how the individual must be given the chance to object to the processing to any processing of their personal data they do not agree to. In a similar vein, the incorporation of the doctrine of consent within the Regulation allows the individual to make determinations in respect of when, where, and under what circumstances their personal data are shared with, and used by, others. The right to be forgotten as contained in Article 17 of the Regulation then allows individuals to demand the deletion of their personal data if they disapprove of how their data are being used by another party and wish to withdraw their consent to the processing thereof, and the right to data portability allows individuals to move their personal data from one third party to another in similar situations.

The key difference between the right of integrity contained within the CDPA and the mechanisms contained within the Regulation considered here is the fact that, unlike the right to integrity, the rights to information and access of personal data, and the rules regarding the individual's consent as well as the right to be forgotten and right to data portability require no "derogatory treatment" of the individual's personal data in order for the individual to invoke them. Neither is there any requirement for the personal data of the individual to be communicated to the public at large before any of these provisions become available. Whilst this difference is notable, however, the key overarching similarity between the two different areas of law is that both are primarily concerned with enhancing individual control by way of statutory rules which can be invoked by the individual as a means of controlling something that is personal to them by way allowing them to object to uses of aspects of their identity to which they do not approve. In the context of both the right to integrity and various data protection rights,

---

[100] *Pasterfield v Denham* [1999] FSR 168, 180.
[101] CDPA 1988 s.80(1), (2). See also: *Confetti Records v Warner Music UK Ltd* [2003] EMLR; *Snow v The Eaton Centre* (1982) 70 *CPR* (2d) 105 (Canada).
[102] *Ibid*
[103] Bently, L. and Sherman, B. (n 57) pg.257.

if these mechanisms are successfully invoked, the uses of the personal thing in question to which the individual objects will be deemed unlawful.

4.4 Discussion

By considering the theoretical underpinnings of the doctrine of moral rights, and by considering the practical implementation of the doctrine by using the law of the United Kingdom as a case in point, we can see there are numerous observable similarities between moral rights and data protection rights. As highlighted above, despite moral rights and data protection rights being concerned with qualitatively different subject matter, they are both plainly concerned with the notion of control and ensuring individuals can exert control over certain things that are somehow personal to them or intrinsically linked to their identity. Both creative works, and personal data, can be accurately described as such.

Whilst personal data and creative works are prima facie qualitatively different in nature, we can see that, between the two different areas of law, the theoretical justifications and rationale for seeking to establish individual control over them are extremely similar. The desire to establish individual control from both moral rights and data protection perspectives is evidently heavily linked to the idea that doing so will allow the individual to manage important aspects of their identity and, concurrently, will provide wider societal benefits through ensuring the accuracy and integrity of certain types of information.

These similarities, however, run deeper than these purely theoretical resemblances. Instead, when looking at the practical implementation of moral rights, we can see there are apparent practical similarities between the two. Not only do some practical implementations of the right of attribution and right of integrity appear to be notably similar in form to a number of initiatives concerned with individual control contained within European data protection law, like the rights of information and access, the right to be forgotten, the right of data portability and the rules regarding consent, insofar as they all represent legal mechanisms by which individuals can attempt to exert a connection to, or restrict the use of, something that is personal to them, but there is another key similarity that can also be identified. Notably, by giving the individual the ability to assert such connections and make such objections, the notions of control as envisaged by both the doctrine of moral rights and data protection law appear to place a heavy emphasis on the individual being a rational and autonomous agent. Both areas of law appear to view the individual as a figure who is presumed to have the capacity to make active and informed choices regarding the use of information or objects that are intrinsically linked to their identity. Whilst, as noted above, there are some doubts as to whether it is appropriate for the law to treat individuals as such, the fact that this is an approach taken by both areas of law is enough to demonstrate an interesting link between the two.

Given the apparent similarities between these two different areas of law and legal scholarship, both of which appear to be concerned with individual control, it can tentatively be concluded that by looking more thoroughly and extensively at how control is envisaged and treated within the doctrine of moral rights, an area of law that has existed for far longer, and is far more developed, than data protection law as we know it today, we might be able to learn more about the true nature of control as contained within data protection law which, as noted previously, is a concept which is poorly-understood and under-developed.

5. Conclusion

The objective of this article was to consider whether the doctrine of moral rights could be used as a basis for understanding the notion of control within European data protection law. Having examined the scholarly literature pertaining to the control of personal data and information, EU policy documents pertaining to individual control of personal data, and some theoretical and practical aspects of the doctrine of moral rights as a part of intellectual property law, it has been possible to draw the following conclusions.

First, with regards to the academic and scholarly literature pertaining to individual control over personal data there is notable confusion as to the true nature and value of control as a concept. Following this, despite the apparent confusion and lack of certainty demonstrated by the academic and scholarly literature, a review of EU policy documents pertaining to the European Data Protection framework reveals that individual control of personal data is a notion which features heavily, and is clearly thought of as a primary means by which a number of regulatory challenges and problems linked to contemporary data-handling practices can be solved or at least guarded against. However, somewhat troubling, the notion of control apparently envisaged by these documents appears to be even more entangled and poorly-understood than that which has been articulated by the academic and scholarly literature.

Whilst it is plainly obvious that the conception of control favoured by EU regulators and lawmakers is one that has considerable individualistic and structural dimensions, by focusing so heavily on issues relating to individual autonomy and capacity in relation to the control of personal data it would appear that questions relating to the true nature, scope, extent and purpose of control in this context have been overlooked. This is unfortunate, as if questions of this nature are not given an appropriate answer, this may be seriously disadvantageous to endeavours to establish the pragmatic and practical elements of control. Clearly there is a real need to engage with these questions in greater depth.

Finally, the third substantive section of the article considered the doctrine of moral rights, a key element of European intellectual property law, another field of law and legal practice concerned with notions of individual control. Here it was identified that not only does the doctrine of moral rights apparently share a number of theoretical foundations with the concept of data protection but, through using the law of the United Kingdom as a case in point, it was shown that the two also share a number of practical similarities. From this, it is possible to draw the tentative conclusion that by looking more deeply at how control is envisaged by the doctrine of moral rights we may be able to more rigorously develop our understanding of control as envisaged by European data protection law, and perhaps come to answers for some of the questions which, as noted above, are currently unanswered.