



ELSEVIER

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

journal homepage: [www.elsevier.com/locate/CLSR](http://www.elsevier.com/locate/CLSR)


---



---

**Computer Law  
&  
Security Review**


---



---



# Our data? An examination of the possible role of individual consent in the regulation of posthumous medical data donation (PMDD)

Henry Pearce

Portsmouth Law School, University of Portsmouth, Anglesea Road, Portsmouth, NH, PO1 3DJ, United Kingdom

## ARTICLE INFO

### Keywords:

Posthumous medical data donation (PMDD)  
Data protection  
Personal data  
Medical data

## ABSTRACT

This article considers the regulation of posthumous medical data donation (PMDD) and examines the extent to which the law should require the opt-in ante-mortem consent of deceased persons for their medical data to be retained and used as part of PMDD initiatives. The article considers arguments on either side of this debate (i.e., pro-consent vs. anti-consent) before tentatively suggesting that, as a general matter, opt-in consent should not be required for medical data of deceased persons to be used for PMDD purposes. It is also proposed, however, that whilst opt-in consent should not be required by law, individuals should be provided with a qualified right through which they can object or “opt out” of their medical data being used in this way.

© 2022 The Authors. Published by Elsevier Ltd.

This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

## 1. Introduction

Previous contributions to the literature have established posthumous medical data donation (PMDD) as the philanthropic notion of donating personal data pertaining to one's health and medical conditions, post-mortem for the purposes of non-commercial medical research.<sup>1</sup> In particular, it has been argued how despite there being many significant benefits to PMDD, notably the way in which it facilitates individual participation in ‘citizen science’ and the development of cures and treatments for some of the most acute known dis-

eases and medical conditions, the law provides scant accommodation for this practice and in some instances may hinder it. Consequently, a new bespoke regulatory framework for PMDD is desirable. Though no attempt to advance a detailed legal solution for PMDD has been made to date, several key issues that would require consideration in the design stages have been identified.<sup>2</sup>

One significant question that warrants investigation relates to the possible role of consent in the regulation of PMDD. Some would likely argue, for instance, that the opt-in consent of a deceased person to whom medical data relate, expressed ante-mortem, be required for such data to be lawfully retained and used as part of PMDD initiatives. Conversely, others would likely argue the law should permit the non-authorized automatic retention and use of such data for PMDD purposes with no consent requirement. This paper aims to raise awareness of this debate by considering arguments on both sides and by offering some normative suggestions as to how this conflict

E-mail address: [henry.pearce@port.ac.uk](mailto:henry.pearce@port.ac.uk)

<sup>1</sup> E Harbina and H Pearce, ‘Your data will never die, but you will: A comparative analysis of US and UK post-mortem data donation frameworks’ [2020] 36 Computer Law & Security Review 105403; E Harbinja, ‘Posthumous Medical Data Donation: The Case for a Legal Framework’ in J Krutzinna and L Floridi (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series. Vol 137 (Springer: Cham 2019).

<sup>2</sup> *Ibid.*

might best be resolved. As with other work in the field, the arguments considered and made here are inspired by medical law and ethics literature pertaining to organ donation.<sup>3</sup>

The paper comprises of five sections. The first section provides an overview of the notion of PMDD. The second section gives a brief outline of the concept of informed consent and explains its significance in the context of PMDD. The third section considers arguments in favour of ante-mortem opt-in consent being required for the medical data of deceased persons to be lawfully retained and utilised as part of PMDD initiatives. The fourth section then sets out arguments which hold that ante-mortem opt-in consent should not form part of any prospective PMDD regulatory framework. Section five then tentatively argues that in light of the arguments considered previously, the law should not require ante-mortem opt-in consent for medical data of deceased persons to be lawfully incorporated into PMDD initiatives, but that the individuals should enjoy a limited right to object to their data being used for such purposes. This, it is suggested, would represent a compromise that would hopefully be acceptable to those on either side of the consent debate. The paper then concludes with a summary of its findings and some suggestions for future research.

## 2. Posthumous medical data donation (PMDD)

The concept of posthumous medical data donation (PMDD) *prima facie* shares many similarities with organ donation, a practice that entails the donation of an individual's organs post-mortem, usually for the purposes of medical research or treatment. This practice is rooted in a philanthropic rationale that recognises the importance of promoting the welfare of others and is widely recognised as being crucial to the development of new medical treatments and therapies.<sup>4</sup> For instance, as highlighted elsewhere, the collation and aggregation of medical datasets is extremely beneficial in terms of developing of personalised medicine, and to the development of entirely new ways of understanding some of the most acute medical conditions currently facing humanity (e.g., cancer).<sup>5</sup>

<sup>3</sup> Many of the arguments considered and made in this paper were inspired particularly by the works of Margaret Brazier, Jonathan Herring, and John Harris. These are referred to and cited throughout.

<sup>4</sup> See: D Shaw, J Gross and T Erren, 'Data donation after death: A proposal to prevent the waste of medical research data' [2016] 17(1) *EMBO Rep* 14-17; E Vayena and J Tasioulas, 'We the Scientists': a Human Right to Citizen Science' [2015] 28 *Philosophy & Technology* 479-485; J Krutzinna, M Taddeo and L Floridi, 'Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data' in J Krutzinna and L Floridi (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series. Vol 137 (Springer: Cham 2019); B Prainsack, 'The Powers of Participatory Medicine' [2014] 12(4) *PLoS Biology*; V Huser and J Ciminho, 'Don't take your EHR to heaven, donate it to science: legal and research policies for EHR post mortem' [2014] 21(1) 8-12.

<sup>5</sup> B Prainsack *Ibid.* See also: R Li et al, 'Electronic health records and polygenic risk scores for predicting disease risk' [2020] 21 *Nature Reviews Genetics* 493-502; N Artzi et al, 'Prediction of gestational diabetes based on nationwide electronic health records' [2020] 26 *Nature Medicine* 71-76; G Taskler et al, 'Opportunities,

However, whilst most nations have bespoke legal regimes pertaining to organ donation, and legal scholarship in this field has expanded considerably over the last few decades, there appears to be no jurisdiction anywhere in the world that operates a bespoke regulatory framework for PMDD, and legal scholarship in this area remains sparse. This is problematic. As noted elsewhere, the absence of legal and regulatory rules pertaining to data governance can often leave individuals and organisations unsure of what rights they have in respect of data in their possession and when, how, and in what circumstances they can or cannot use those data.<sup>6</sup> In the context of PMDD this lack of certainty can result in a failure to fully exploit data stored in public health records (e.g., such as those held by the NHS, in the UK), leading to huge opportunity costs and the impediment of medical research.<sup>7</sup>

Previous literature in the field has highlighted how in some jurisdictions limited policy options regarding the posthumous donation of medical data occasionally exist.<sup>8</sup> So far, however, no region or jurisdiction has established a comprehensive regulatory framework through which individuals can proactively donate their medical data for research or therapeutic purposes in a way comparable to organ donation.<sup>9</sup> In the UK, the most significant legal rules pertaining to the usage of individuals' personal data<sup>10</sup> are primarily set out in the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR). Neither the DPA nor the UK GDPR govern the processing (i.e. more or less any imaginable use) of the personal data of deceased persons.<sup>11</sup> Recital 27 of the UK GDPR explicitly excludes the personal data of the deceased from its scope, and s.3(2) DPA makes it clear that its terms apply to the data of "living individuals" only. The upshot of this is that data protection rules and rights pertaining to an individual's personal data in life cease to apply upon the individual's death. Notably, the processing of the personal data of deceased persons does not need to comply with the data protection principles,

Pitfalls, and Alternatives in Adapting Electronic Health Records for Health Services Research' [2021] 41(2) *Medical Decision Making* 133-142; L Beesley et al, 'The emerging landscape of health research based on biobanks linked to electronic health records: Existing resources, statistical challenges, and potential opportunities' [2020] 39(6) *Statistics in Medicine* 773-800; A Callahan, NH Shah and JH Chen, 'Research and Reporting Considerations for Observational Studies Using Electronic Health Record Data' [2020] 172 *Annals of Internal Medicine* 79-84.

<sup>6</sup> This will often particularly be the case with datasets held by public authorities, including those responsible for maintaining public health records. On this issue, see: M Khayyat and F Bannister, 'Open Data Licensing: More than meets the eye' [2015] 20(4) *Information Polity* 231-252; N Korn and C Oppenheim, 'Licensing Open Data: A Practical Guide' [2011] *JISC*.

<sup>7</sup> J Krutzinna, M Taddeo and L Floridi (n 4). See also: E Harbinja and H Pearce (n 1).

<sup>8</sup> *Ibid.*

<sup>9</sup> *Ibid.*

<sup>10</sup> The term "personal data" is defined expansively by Art.4(1) UK GDPR as "...any information relating to an identified or identifiable natural person ('data subject')".

<sup>11</sup> The term "processing" is also defined expansively by Art.4(2) UK GDPR as "...any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means...".

nor does it require a legitimising basis.<sup>12</sup> Significantly, as is returned to below, the consent of the individual is not required for the processing of their personal data post-mortem.<sup>13</sup>

Thus far, we have established two things. First, that PMDD is an important and valuable philanthropic endeavour. Second, that the UK's existing legal framework neither recognises nor facilitates this practice. This raises the question: if existing legislation and regulatory mechanisms do not adequately support this practice, are new bespoke legal rules required for the achievement of this goal? This is another notion discussed in recent literature, where it has been suggested that for PMDD to achieve its maximum potential fresh legal and/or regulatory interventions will likely be required.<sup>14</sup> However, the successful construction of a bespoke PMDD regulatory regime would require engagement with several challenging questions. One of the most significant of these questions relates to the role of the individual, and the extent to which their consent, authorisation, or preferences more generally, should play a part in any PMDD regulatory framework.<sup>15</sup>

### 3. Consent

The doctrine of informed consent, with its roots in medical law and ethics, was originally explained in legal casebooks as originating from the need for patients to be able to “take courage” as they confronted the predicament of pre-anaesthetic medicine.<sup>16</sup> Over the course of the last few centuries a much broader interpretation of the concept has developed. It is now commonly understood that the act of giving consent can be described as the agreement of an individual, or group of individuals, to grant permission for something to happen, or something to be done, to their person or their property. In most contexts, therefore, the primary function of consent is to neutralise or legitimise actions that, in the absence of an individual's wishes, would normally be considered wrong.<sup>17</sup> The fundamental principle underlying the doctrine is a right of self-determination: the principle of autonomy of the person.<sup>18</sup> Autonomy, therefore, and the fortification thereof, is widely accepted as being the cornerstone

of consent's rationale.<sup>19</sup> Autonomy, however, is an expansive term. As noted by Dworkin:

“It is equated with dignity, integrity, individuality, independence, responsibility, and self-knowledge. It is identified with qualities of self-assertion, with critical reflection, with freedom from obligation, with the absence of external causation, with knowledge of one's own interests.”<sup>20</sup>

In a similar vein, Raz suggests:

“The ideal of personal autonomy...holds the free choice of goals and relations as an essential ingredient of individual well-being. The ruling idea behind the ideal of personal autonomy is that people should make their own lives.”<sup>21</sup>

In recent decades, consent, as a vehicle through which individual autonomy can be protected, has assumed an increased role in numerous areas of law.<sup>22</sup> Notable examples include the incorporation of consent in data protection law, and laws relating to organ donation. Within data protection law, for instance, consent has assumed a role as a major means through which the processing of personal data can be made lawful.<sup>23</sup> In a similar vein, organ donation legislation often prohibits the extraction of bodily material without the consent, or at least the authorisation, of a relevant individual.<sup>24</sup> In both contexts consent acts as a mechanism through which individuals can exercise autonomy and control in relation to commodities which are intrinsically linked to their identities and personhood: their personal data and their organs. Particularly, it allows individuals to authorise uses of their personal data and their organs that in the absence of their consent would be unlawful or otherwise illegitimate.

As has been argued elsewhere, notably by Harbinja, there are convincing reasons for why individuals should, as a gen-

<sup>19</sup> It should be noted, however, that despite this being the prevailing view, some scholars have challenged this assertion. See, for example: L White, ‘Understanding the Relationship Between Autonomy and Informed Consent’ [2013] 47 *The Journal of Value Inquiry* 483-491.

<sup>20</sup> G Dworkin, ‘The theory and practice of autonomy’ (Cambridge: Cambridge University Press 1988) 6.

<sup>21</sup> J Raz, *The Morality of Freedom* (Oxford: Clarendon 1986) 369. For a detailed discussion on the finer conceptual aspects of autonomy, see: J Satre, *Existentialism is a Humanism* (New York: Philosophical Library 1946); M Friedman, *Autonomy, Gender, Politics* (Oxford: Oxford University Press 2003); A Ingram, *A Political Theory of Rights* (Oxford: Oxford University Press 1994); AC Grayling, *The Heart of Things: Applying Philosophy to the 21<sup>st</sup> Century* (London: Weidenfeld & Nicolson 2005).

<sup>22</sup> For an overview for the different areas of law into which the doctrine of informed consent has been incorporated, see: S Hansson, ‘Informed Consent out of Context’ [2006] 63(2) *Journal of Business Ethics*.

<sup>23</sup> On the role of consent within data protection law, see: E Kosta, *Consent in European Data Protection Law* (Boston: Martinus Nijhoff Publishers 2013).

<sup>24</sup> For instance, in the UK Section 1 of the Human Tissue Act 2004 specifies that it is lawful to remove, store, or use “human material” from deceased and living persons provided that “necessary consent” has been obtained from the relevant individual(s). In the USA Section 4(1) of the Uniform Anatomical Gift Act 2006 allows people to authorise the donation of their organs by way of making an “anatomical gift”.

<sup>12</sup> See: Arts 5-11 GDPR.

<sup>13</sup> As per Art.6(a) GDPR, if an individual (i.e., data subject) gives consent to the processing of their personal data for one or more specific purposes, this is one way through which the processing of that individual's personal data can be rendered lawful. For an overview of all the different legal bases for personal data processing set out in Art.6 GDPR, see: S Stalla-Bourdillon, H Pearce, and N Tsakalakis, ‘The GDPR, a Game Changer for Electronic Identification Schemes? The Case Study of Gov.UK Verify’ [2018] 34(4) *Computer Law & Security Review* 784-805.

<sup>14</sup> E Harbina and H Pearce (n 1).

<sup>15</sup> *Ibid.*

<sup>16</sup> M Kirby, ‘Informed Consent: What Does It Mean?’ [1983] 9(2) *Journal of Medical Ethics* 69.

<sup>17</sup> G Fletcher, *Autonomy, Consent and the Law*, (Routledge 1996) 109.

<sup>18</sup> *Ibid.* See also: A Goldsworth, ‘Informed Consent in the Genetic Age’ [1999] *Cambridge Quarterly of Healthcare Ethics* 393; A Maclean, ‘Now You See It, Now You Don't: Consent and the Legal Protection of Autonomy’ [2000] 17(3) *Journal of Applied Philosophy* 277.

eral matter, be provided with legal mechanisms through which they can exercise control over their personal data post-mortem (e.g., by requiring consent of deceased persons for any future uses of their personal data to be lawful).<sup>25</sup> This is a notion now widely referred to as “post-mortem privacy”, and is discussed in greater detail below.<sup>26</sup> With this being the case, it might be assumed that the arguments for individuals being able to control their personal data post-mortem in a general sense should logically extend to medical data that may be relevant to PMDD initiatives. However, this issue is not as straightforward as it might initially appear. In the context of PMDD, where the medical data of deceased persons may have a high latent value, significant conflicts of interest will likely arise in relation to future uses of such data. This is mainly due to the way in which potential uses of such data may significantly contribute to the development of new medical treatments and therapies for serious medical conditions. With this being the case, we must question how, whether, and to what extent consent should play a role in any PMDD regulatory framework. Given how in November 2020 the European Commission unveiled a proposal for a Data Governance Act which, amongst other things, proposes the construction of an authorisation framework for secondary uses of certain types of data, including non-personal data (i.e., data relating to deceased persons), this is now a particularly salient question.<sup>27</sup> The subsequent sections consider arguments for and against the incorporation of the doctrine of consent in prospective PMDD regulatory frameworks.

## 4. Pro-consent arguments

This section sets out a range of arguments as to why consent should be required by law for medical data of deceased persons to be incorporated into PMDD initiatives. These arguments are generally rights-based and built around the notions that living persons have legitimate claims to determine what happens to their medical data after their death, and that the bereaved family and friends of the deceased have legitimate claims to be protected from emotional distress and psychiatric harm arising from the deceased’s death.

### 4.1. Autonomy, post-mortem privacy, and informational self-determination

The first of the pro-consent arguments considered here relates to autonomy, and the growing importance of individuals being able to control how their personal data are collected and used by others post-mortem. A useful starting point for considering this argument is to note that overriding a deceased person’s ante-mortem wishes regarding their personal data as

if they were of no account is arguably to deeply disrespectful to that person. This is not to say that a person will be disrespected when any of their wishes are ignored, but that to ignore wishes regarding fundamental aspects of their identity and personhood (e.g., such as wishes relating to their personal data) would be to disrespect them. As noted elsewhere, when put this way, the idea of disrespect appears to closely relate to certain conceptions of autonomy.<sup>28</sup> Autonomy, as set out above, is literally “self-rule”, and while personal data, including medical data, are not in themselves “the self”, they are at least very closely related, and self-rule implies control. Against this background, it is increasingly argued that, as the capabilities and pervasiveness of digital and analytical technologies continue to rapidly develop, the careful stewardship of personal data, which can, in some sense, be said to be a rich reflection of an individual’s personhood and identity, is becoming ever more important.<sup>29</sup> As a consequence, perhaps to prevent the revealing of information that would cast them in a negative light, individuals now have a greater interest in being able to control their personal data post-mortem than at any point in history. As noted by Edwards and Harbinja:

“More than ever before, “ordinary people” leave digital relics which may be highly personal and intimate, and are increasingly preserved and accessible in a large volume after death.”<sup>30</sup>

Here, Edwards and Harbinja refer specifically to personal data that are stored and accessible online, for example through social media platforms. However, their statement is also applicable to a person’s medical data. For instance, the quantity, capability, and durability of digitally stored personal data, such as medical data stored as part of an electronic health record (EHR), arguably challenges the traditional view that privacy, data protection, and other rights pertaining to informational self-determination end at death.<sup>31</sup>

In a general sense, justifications for extending such rights beyond death can be derived from scholarship in several different fields, particularly those concerned with legal notions of property and personality. Some scholars, for instance, have highlighted the difficulty in identifying precisely when death legally occurs and have questioned whether legal personality either does, or should, terminate upon death.<sup>32</sup> Others have highlighted how aspects of other areas of law, such as intel-

<sup>28</sup> See: J Wilkinson, ‘Individual and Family Decisions about Organ Donation’ [2007] 24(1) *Journal of Applied Philosophy*.

<sup>29</sup> See, for example: JC Buitelaar, ‘Post-mortem privacy and informational self-determination’ [2017] 19 *Ethics and Information Technology* 129-142.

<sup>30</sup> L Edwards and E Harbinja, ‘Protecting post-mortem privacy: Re-considering the privacy interests of the deceased in a digital world’ [2013] 32(1) *Cardozo Arts & Entertainment Law Journal* 135.

<sup>31</sup> A Lopez, ‘Posthumous Privacy, Decedent Intent, and Post-Mortem Access to Digital Assets’ [2016] 24 *George Mason Law Review*.

<sup>32</sup> See: N Naffine, ‘When Does the Legal Person Die? Jeremy Bentham and the ‘Auto-Icon’ [2000] 25 *Australian Journal of Legal Philosophy* 79-95; R Tur, ‘The ‘Person’ in Law’ in A Peacocke and G Gillett (eds) *Persons and Personality: A Contemporary Enquiry* (Oxford: Basil Blackwell 1987) 116-129; D Erdos, ‘Dead ringers? Legal persons and the deceased in European data protection law’ [2021] 40 *Computer Law & Security Review* 105495.

<sup>25</sup> E Harbinja, ‘Post-mortem privacy 2.0: theory, law and technology’ [2017] 31(1) *International Review of Law, Computers & Technology* 26-42.

<sup>26</sup> *Ibid.*

<sup>27</sup> See: European Commission, Proposal for a Regulation on European data governance (Data Governance Act), COM(2020) 767. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>.

lectual property law, also protect the integrity of individual personhood beyond death. Harbinja, for instance, highlights how in some jurisdictions moral rights, as a personal aspect of copyright, extend on the death of a creator of an artistic work either perpetually (e.g., in France) or for a lesser period with an option of waiving these rights (e.g., in the US and the USA).<sup>33</sup> This, she contends, demonstrates how aspects of personality, such as dignity, integrity and autonomy, survive death. As privacy and data protection rights are intended to protect these values, there is no good reason, she argues, why other legal rights designed to protect them (e.g., moral rights) should extend beyond death and privacy and data protection rights should not.<sup>34</sup>

Alternatively, various observers have argued that a person's property represents a manifestation of their personality and free will.<sup>35</sup> Others have further argued how freedom of testation (i.e., the ability of deceased persons to determine what happens to the property and assets post-mortem) can be characterised as a manifestation of autonomy. Thus, if property is an extension of an individual's personality and the same can be said of freedom of testation, which is guaranteed to some extent by the laws of most developed countries, a necessary implication of a person's property transcending death is that their personality must also transcend death. Ergo, legal rules designed to protect core aspects of an individual's personality (e.g., dignity, integrity, and autonomy), such as those relating to privacy and data protection, should also extend beyond death.

To summarise, the crux of the arguments considered in this section is that people should be free to create and shape their lives, and that the law should facilitate and protect their ability to do so. They are arguments that hold that the ability of individuals to create and shape their lives can and should extend to both how they die, and what happens to them and aspects of their personhood and identity (such as their personal data) after death. Failing to respect these wishes would not only be disrespectful to the individual in question but would infringe their autonomy. Were the law to require individuals' opt-in consent for medical data to be retained and utilised as part of any PMDD initiative, this would be one way through which the protection of the autonomy and post-mortem privacy of the deceased could be achieved.

#### 4.2. Conscientious beliefs

Another pro-consent argument links to freedom of conscience. A useful starting point for its consideration is the right to freedom of thought, conscience, and religion, which is expressly protected through Article 9 of the European Convention on Human Rights (ECHR). This right establishes that

not only does every person have a right to choose and change their beliefs, but that they have a right to both publicly and privately manifest their beliefs in worship, teaching, practice, and observance. In other words, it guarantees the right of the individual to have and to exercise conscientious beliefs. Ellis succinctly summarises conscientious beliefs as:

“...beliefs and practices, which are not merely important to people, but important because, in light of their content, they are regarded as somehow demanded of them. This would extend to moral, political and, perhaps, some aesthetic beliefs as well as religious ones.”<sup>36</sup>

Of particular interest in the context of PMDD are conscientious beliefs pertaining to data protection and privacy. It is plausible, for instance, that in addition to considerations relating to privacy, autonomy and self-determination some individuals may object to their personal data being used for PMDD purposes for other conscientious reasons. In this regard it is important to note that religions such as Islam and Judaism place great importance on data protection and privacy, and particularly the ability of individuals to control information about themselves. For instance, as noted by Hayat, according to the standards of Sharia (i.e., religious laws that form part of the Islamic tradition) private life, private information and the affairs of the individual are left to the individual's recognition as part of their “private domain”, and no one, not even the state, has the authority to interfere with anything falling within this domain in anything other than exceptional circumstances.<sup>37</sup> In a similar vein, Bamberger and Mayse have remarked on how Judaism not only views privacy as an important individual value, but as a prerequisite for a functioning society.<sup>38</sup> They note how, according to Jewish doctrine, failing to protect privacy can:

“...rend the fabric of society—with severe implications for its members.”<sup>39</sup>

Golinkin goes further, and suggests that halakah (i.e., the totality of laws and ordinances that have evolved since biblical times to regulate religious observances and the daily life and conduct of Jewish people) forbids the usage of confidential information about a person without the express permission of the person in question.<sup>40</sup> To this end it is conceivable that some individuals may have religious, or other conscientious, objections to their personal data being used as part of PMDD initiatives so to prevent information that would pre-

<sup>33</sup> E Harbinja (n 28).

<sup>34</sup> *Ibid.*, See also: E Harbinja, ‘Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?’ [2013] 10(1) SCRIPTed.

<sup>35</sup> See, for example: GWF Hegel, *Elements of the Philosophy of Right* (Oxford: Oxford University Press 1967); J Penner, *The Idea of Property in Law* (Oxford: Oxford University Press 1997); GS Alexander and EM Peñalver, *An Introduction to Property Theory* (Cambridge: Cambridge University Press 2012); MJ Radin, ‘Property and Personhood’ [1982] 34 *Stanford Law Review* 957-1015.

<sup>36</sup> A Ellis, ‘What is special about religion?’ [2006] *Law & Philosophy* 219-41.

<sup>37</sup> M Hayat, ‘Privacy and Islam: From the Quran to data protection in Pakistan’ [2007] 16(2) *ICTL* 137-148. See also: M Lurbis and M Kartiwi, ‘Privacy and trust in the Islamic perspective: Implication of the digital age’ [2013] *IEEE*.

<sup>38</sup> K Bamberger and A Mayse, ‘Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age’ [2021] *Journal of Law and Religion* (forthcoming). See also: A Cohen, ‘Privacy: A Jewish Perspective’ [1981] 1(1) *The Journal of Halacha* 53-102.

<sup>39</sup> *Ibid.*

<sup>40</sup> D Golinkin, ‘A Responsum Regarding the Right to Privacy’ [1996] 48(3) *Conservative Judaism* 10-13.

fer to remain private becoming publicly known.<sup>41</sup> Whilst such beliefs might be dismissed as trivial or self-indulgent by non-believers, the frustration of such beliefs and preferences can be acutely painful for those who hold them.<sup>42</sup> Pursuant to this, McGuinness and Brazier note how conscientious beliefs have a normative force and compel individuals to act a certain way, effectively removing their choice to act any other way.<sup>43</sup> In their view, telling such people that their wishes are not deserving of respect simply because they are not held by others is unsatisfactory and inappropriate. Forcing people to abandon or modify these beliefs, or frustrating their freedom to exercise them, requires a level of sacrifice that is qualitatively different, and more emotionally demanding, than other common situations in which competing interests must be weighed.<sup>44</sup> They further highlight how a person having knowledge that their conscientious beliefs and objections may not be respected post-mortem can cause them torment and mental anguish whilst they are still alive.<sup>45</sup> In other words, to many, knowledge of how they and their wishes will be treated after death will affect their welfare in life.

With this being the case, failure to respect a person's wishes (or objections) regarding post-mortem uses of their medical data may have the potential to compromise their freedom of conscience. By the same token, it can also be argued that simply respecting the wishes of deceased persons regarding their medical data should be considered a worthwhile endeavour in itself regardless of any other ancillary justifications for doing so (e.g., to preserve individual autonomy). Accordingly, as an opt-in consent requirement would provide individuals with a mechanism through which their conscientious beliefs could be protected, this is another possible justification for why opt-in consent should always be required as a general matter for medical data of deceased persons to be retained and used for PMDD purposes.

#### 4.3. Relational and genetic privacy

Relational privacy is a variant of informational privacy (i.e., the ability to determine how information relating to oneself is collected and used by others) which is applicable to situations in which interests in the flow and control of information lie with a collective group, rather than with an individual.<sup>46</sup> An example of such a situation might be a family dinner at which many relatives are present. In this situation some family members

may jointly realise that the disclosure of certain information to a particular relative will likely result in conflict, and so collectively they decide not to broach certain topics of conversation. No single family member can unilaterally realise the goal of ensuring the occasion remains harmonious. This can only be achieved through all family members observing the relevant strictures on the flow of information. Concurrently, if one individual divulges information that causes conflict it will not merely be that individual who suffers the ill-effects, but the family collective.<sup>47</sup> This phenomenon is also relevant to situations where a group of individuals may be affected by disclosure or uses of data relating to a deceased individual. A summary of this paradigm is provided by Bikker, who notes:

“Relational privacy has its foundations in two premises. Individuals maintain their relational status with relatives even after those family members dies. Secondly, although the dead no longer have a privacy interest in personal information about themselves, their surviving relatives who wish to cherish their remedies may well do.”<sup>48</sup>

Though Bikker addresses relational privacy in the context of disaster victim identification,<sup>49</sup> it is a notion that is also salient in the context of digitally stored personal data, and particularly medical data and PMDD.<sup>50</sup> For instance, PMDD analyses of a deceased person's medical data may reveal information of which the person's close relatives were previously unaware. Were this information to become known it could potentially have significant negative effects on both the relatives' grieving process and their emotional well-being. For example, post-mortem analyses of the deceased's medical data may reveal that they were suffering from a sexually transmitted disease. This information might then reveal further information relating to the deceased's ante-mortem behaviours that may cause distress to their relatives, such as the occurrence of an extra-marital affair. Alternatively, post-mortem analyses of the deceased's medical data may reveal genetic information pertaining to the health of people who are still alive. To this end, in the PMDD context relational privacy interests may overlap with interests linked to genetic privacy: the notion that individuals should be able to restrict uses of data pertaining to their gene sequence so to prevent the manifestation of privacy harms relating either to themselves or to others.<sup>51</sup> For instance, PMDD uses of medical data might reveal that a

<sup>41</sup> For instance, individuals may worry that usage of their personal data for PMDD purposes may reveal diagnoses for medical conditions illness to which societies have historically attached stigmas (e.g. sexually transmitted diseases and mental illnesses).

<sup>42</sup> On this issue, see: A Sheikh and AR Gatrud, *Caring for Muslim Patients* (Abingdon: Routledge 2001).

<sup>43</sup> S McGuinness and M Brazier, 'Respecting the Living Means Respecting the Dead too' [2008] 28(2) *Oxford Journal of Legal Studies* 306.

<sup>44</sup> *Ibid* 307.

<sup>45</sup> *Ibid*.

<sup>46</sup> Y Ma, 'Relational Privacy: Where the East and West could meet' [2019] 56(1) *Proceedings of the Association for Information Science and Technology* 196-205; S Bannerman, 'Relational privacy and the networked governance of the self' [2019] 22(14) *Information, Communication & Society* 2187-2202.

<sup>47</sup> RH Sloan and R Warner, 'Relational Privacy: Surveillance, Common Knowledge, and Coordination' [2017] 11(1) *University of St. Thomas Journal of Law and Public Policy* 1.

<sup>48</sup> J Bikker, 'Disaster victim identification in the information age: The use of personal data, post-mortem privacy and the right of the victim's relatives' [2013] 10(1) *SCRIPTed* 60. See also: E Kasket, 'Access to the Digital Self in Life and Death: Privacy in the Context of Posthumously Persistent Facebook Profiles' [2013] *SCRIPTed*; J Berg, 'Grave secrets: Legal and ethical analysis of postmortem confidentiality' [2001] *Connecticut Law Review* 81-122.

<sup>49</sup> On this issue, see also: C Emery, 'Relational Privacy – A Right to Grieve in the Information Age: Halting the Digital Dissemination of Death-Scene Images' [2011] 42 *Rutgers Law Journal* 765.

<sup>50</sup> See: U Reviglio and R Alunge, "I Am Datafied Because We are Datafied": an Ubuntu Perspective on (Relational) Privacy' [2020] 33 *Philosophy & Technology* 595-612; RH Sloan and R Warner (n 59).

<sup>51</sup> L Gostin, 'Genetic Privacy' [1995] 23(4) *Journal of Law, Medicine & Ethics* 320-330; E Clayton et al, 'The law of genetic privacy: ap-

deceased person either had an undiagnosed serious inheritable disease, or that they were not the biological parent/child of another person.<sup>52</sup> Either scenario could cause significant distress to surviving relatives of the deceased person. With this being the case, it is arguable that the law should provide mechanisms through which affected persons could be protected from harms of this sort. One way through which this might be achieved would be for the law to require opt-in consent prior to the medical data of deceased persons being retained and utilised as part of PMDD initiatives.

#### 4.4. Trust

The final argument considered here relates to trust. Put simply, suggestions that consent should not be required for medical data to be posthumously donated as part of PMDD initiatives, such as those considered below, are necessarily predicated on the notion that there would be sufficient trust in the personnel and institutions responsible for retrieving, storing and processing any data involved. At a minimum this would necessarily require us to have confidence not only in medical practitioners explaining fully and openly why and for what purposes our medical data were to be collected post-mortem, but confidence in the institutions operating PMDD schemes to store the data securely and for specific limited purposes (i.e., for the sake of medical education and/or research). Observers have suggested, however, that the only way of developing levels of trust required for PMDD schemes to be viable would be through the construction of democratically controlled non-profit personal data cooperatives which do not presently exist.<sup>53</sup>

#### 4.5. Discussion

This section of the paper set out several potential arguments as to why opt-in consent should be required for the incorporation of medical data of deceased persons into PMDD initiatives to be lawful. These arguments neither attempt to undermine the value of PMDD initiatives, nor contest how the collection and analysis of medical data of deceased persons has the potential to make significant contributions to the development of medical research. Instead, they assert that for numerous reasons individuals have strong claims to be able to control post-mortem uses of their medical data. They are ar-

guments that recognise and acknowledge that we live in communities where fundamental values of individuals can drastically differ, and that those with contrasting views and interests should respect the views and interests of others. In other words, these arguments hold that it would be no more acceptable for individuals with strong commitments to medical science and communal interests (e.g., those who believe that consent should not be required for the posthumous donation of medical data) to impose their views on others than it would be for individuals with a strong commitment to ensuring post-mortem control of medical data to do the same. The next section of the paper highlights how as compelling as these arguments may prima facie seem, it is unlikely that they will be universally accepted, and that others will have strong opposing views.

guments that recognise and acknowledge that we live in communities where fundamental values of individuals can drastically differ, and that those with contrasting views and interests should respect the views and interests of others. In other words, these arguments hold that it would be no more acceptable for individuals with strong commitments to medical science and communal interests (e.g., those who believe that consent should not be required for the posthumous donation of medical data) to impose their views on others than it would be for individuals with a strong commitment to ensuring post-mortem control of medical data to do the same. The next section of the paper highlights how as compelling as these arguments may prima facie seem, it is unlikely that they will be universally accepted, and that others will have strong opposing views.

## 5. Anti-consent arguments

This section of the paper considers several arguments that may be invoked in opposition to suggestions that consent should play a prominent role in any PMDD regulatory framework. Two major strands of argument are considered. The first strand is referred to as “data communitarian arguments”. The second strand is referred to as “broader ethical arguments.”

### 5.1. Data communitarian arguments

The first category of anti-consent argument considered here is referred to as “data communitarian arguments”.<sup>54</sup> This term has been chosen as the arguments presented here mesh closely with communitarianism, a social philosophy that maintains human entities are largely shaped by their participation in constitutive communities, and that as individuals we are obliged to prioritise providing support to the communities that give meaning to our lives over purely individualistic goals and objectives.<sup>55</sup> To this end, the arguments presented here challenge the extent to which it is appropriate for us to describe our personal data, and particularly our medical data, as “ours”, and the extent to which the law should indulge such notions in the context of PMDD.<sup>56</sup>

One way of introducing this category of arguments is to start with a question: are your personal data yours? Though data protection law in Europe and the UK does not formally grant individuals proprietary interests in their personal data, debate persists as to whether individuals enjoy such interests

plications, implications, and limitations’ [2019] 6(1) *Journal of Law and the Biosciences* 1-36.

<sup>52</sup> J Bikker (n 60). On this issue, see also: JR Goldim and S Gibbon, ‘Between personal and relational privacy: understanding the work of informed consent in cancer genetics in Brazil’ [2015] 6 *Journal of Community Genetics* 287-293.

<sup>53</sup> See: E Hafen, ‘Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health’ in J Krutzinna and L Floridi (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series. Vol 137 (Springer: Cham 2019). See also: A Fong, ‘The role of app intermediaries in protecting data privacy’ [2017] 25(2) *International Journal of Law and Information Technology* 85-114; H Richter and P Slowinski, ‘The Data Sharing Economy: On the Emergence of New Intermediaries’ [2019] 50 *International Review of Intellectual Property and Competition Law* 4-29.

<sup>54</sup> The arguments made here are largely inspired by those made in relation to organ donation by Herring and Chau. See, particularly: J Herring and PL Chau, ‘My Body, Your Body, Our Bodies’ [2007] 15(1) *Medical Law Review* 34-61.

<sup>55</sup> See: H Tam, *Communitarianism* (London: Palgrave 1998). See also: D Bell, *Communitarianism and Its Critics* (Clarendon 1993); A Etzioni, *Communitarianism*. in K Christensen and D Levinson (eds), *Encyclopedia of Community: From the Village to the Virtual World* (Sage 2003) 224-228; R Burke, ‘The Case for a Radical Moral Communitarianism’ [2014] 12(3) *British Journal of Community Justice* 5-18.

<sup>56</sup> To some extent the arguments made here may to some extent also apply to the personal data of living persons. A detailed examination of this issue is, however, beyond the scope of this paper.

in everything but name, and/or whether such an arrangement would be desirable.<sup>57</sup> However, irrespective of these debates, there appears to be a widely held belief that our personal data are, to some extent at least “ours” in the sense that they correspond to, and reveal, intrinsic aspects of our identities. A common response to this question, therefore, might be “Of course my *personal* data are mine; who else’s *could* they be?”

Responses of this sort may be inspired by data protection law’s nomenclature. Both the GDPR and UK GDPR make it clear, for instance, that their main purpose is to establish rules, conditions, and rights in relation to the processing of data that are “personal”, with personal data being defined as any information relating to an identified or identifiable “individual”.<sup>58</sup> The use of this terminology is significant. Though neither the GDPR nor UK GDPR formally confer proprietary interests in personal data,<sup>59</sup> the notion that information relating to an individual is “personal” to that individual is suggestive of that individual having a default entitlement to control that information which *prima facie* supersedes competing interests. In other words, although this wording does not engender individual ownership of personal data, it nonetheless allows and encourages the individual to lay claim to that information and say “that’s mine”, and potentially exclude others from the use of that information. This is a position that is reflected in the substantive provisions of the GDPR and UK GDPR, the jurisprudence of the CJEU,<sup>60</sup> and in EU policy rhetoric.<sup>61</sup> However, the idea that certain types of data are purely “personal”, and that we as individuals should be *de facto* entitled to exert sovereignty over information that relates to us because it is somehow “ours”, is arguably increasingly dubious.

There are at least two claims that can be used to challenge suggestions that personal data (i.e., data that relate to an identified or identifiable individual), including medical data, are “ours”, and that because they are nominally “personal” we should enjoy default sovereignty over them. The first is that our personal data are inevitably interconnected with the personal data of others and attempts to derive meaning from our personal data will often necessarily depend on the personal data of others if they are to be successful. The second is that our personal data are constantly interacting with, and are constantly shaped by, the world around us. A person’s personal data is not a static commodity and is always in a constant state of flux, change, and evolution. Both claims can be used

to support the argument that the idea of nominally “personal” data, which exclusively represent a single person’s identity, is false, and thus form the basis for the argument that the law should not indulge the idea that an individual should be presumed to enjoy a default entitlement to control uses of such data that supersedes competing interests in those data (e.g., by requiring an individual’s opt-in consent for their medical data to be posthumously collected and utilised as part of PMDD initiatives).

#### 5.1.1. Data interconnection

Our personal data are inevitably and inextricably interconnected with the personal data of others in several notable ways. The first example of interconnection occurs at the time a person is born. Specifically, the personal data of a new-born child is necessarily interconnected with the personal data of the mother, and potentially with the personal data of several other people.<sup>62</sup> This is demonstrated in numerous ways. The most obvious of these is the way in which data are recorded on birth certificates. In the UK, for instance, the births of all new-born children must be entered in the national birth register.<sup>63</sup> Entry to the register requires the issuing of a birth certificate, a document containing, amongst other things, the full name of the person born, the date on which they were born, and the location where they were born. In addition to this information, which pertains exclusively to the new-born person in the sense that this information only reveals information about the person themselves (i.e., that the new-born person has a name, and was born at a specific time in a specific location), other information is also recorded. Notably, the full name of the mother, the mother’s place of birth, the mother’s occupation, the mother’s usual address, the father’s full name (if known), and the father’s occupation.<sup>64</sup> An effective way of highlighting the significance of this is through an illustrative example. Imagine Person A is born, and Persons B and C are Person A’s biological parents. A fully completed birth certificate with all the above information would, therefore, reveal the following:

- Person A is the child of Person B and Person C.
- Person B and Person C are the parents of Person A.
- The conception and birth of Person A was the result of sexual activities engaged in by Person B and Person C approximately nine months prior to Person A’s birth.

So, whose personal data is this? Is the fact that Person A is the child of Persons B and C the personal data of Person A, Person B or Person C? Is the fact that Persons B and C shared a sexual relationship resulting in the birth of Person A the personal data of Person A, Person B or Person C? The answer is that this information is the personal data of all three people. It is the personal data of Person A, Person B and Person C, in that it relates to all three, and yet it is neither uniquely nor exclusively “personal” to any of them. In a similar vein, the processing of personal data relating to the health and well-being

<sup>57</sup> See: H Pearce, ‘Personality, property and other provocations: exploring the conceptual muddle of data protection rights under EU law’ [2018] 4(2) European Data Protection Law Review 784-805.

<sup>58</sup> Article 4(1) GDPR and Article 4(1) UK GDPR.

<sup>59</sup> On this issue, see: H Pearce (n 70).

<sup>60</sup> For instance, in *Rynes* the CJEU held that using CCTV equipment attached to a building to record footage of individuals who made use of an adjoining public footpath would not be lawful unless the operators of the equipment satisfied one of the lawful bases for personal data processing set out in Article 6 of the Data Protection Directive. *Rynes* (Case C-212/13) ECLI:EU:C:2014:2428.

<sup>61</sup> For instance, in a 2011 speech, the Vice-President of the European Commission, Neelie Kroes, spoke at length about how enhancing individual control over personal data was vital for reinforcing trust and confidence in online services. See: N Kroes, Online privacy – reinforcing trust and confidence [2011] Online Tracking Protection & Browsers Workshop SPEECH/11/461.

<sup>62</sup> On the inter-relational nature of personal data generally, see: D Erdos (n 35).

<sup>63</sup> See: Births and Deaths Registration Act 1953.

<sup>64</sup> *Ibid.*



of a new-born child can directly shape and influence the personal data of others, notably the parents of the child. Consider the following scenario:

Person A gives birth to Person B.

Person B is, shortly after birth, diagnosed with a serious heart condition. This is recorded in a hospital record (i.e., Person B's personal data is compiled and stored).

Person A is then told about Person B's diagnosis (i.e., the personal data of Person B is communicated to Person A).

Knowledge of Person B's diagnosis (i.e., knowledge of the personal data of Person B) causes Person A to experience psychiatric harm, necessitating medical treatment.

Details of Person A's condition and treatment are then recorded in a hospital record (i.e., Person A's personal data is compiled and stored).

In this scenario, the condition of the personal data of Person A is directly influenced and shaped by the personal data of Person B and the processing thereof. The fact that Person A required treatment for psychiatric harm (i.e., information that would constitute the personal data of Person A) has been caused by Person A becoming aware of the personal data of Person B (i.e., the fact that Person B has a serious heart condition). The personal data recorded in relation to Person A is, therefore, necessarily interconnected with, and shaped by, the personal data of Person B. This phenomenon will extend well beyond the time shortly after a child is born. The continued interactions between parent and child will inevitably affect the personal data of both parties. For instance, the decision of a parent regarding where to send the child to school will shape and influence location data relating to the child. Conversely, if the child requires specific care needs, the parent may need to pursue new employment opportunities to pay for such care, necessitating a shaping and altering of data pertaining to the parent's employment and financial statuses.

The relationship between parent and child is a prime example of how the personal data of one person can influence and shape the personal data of another. However, it is not just in interactions between parent and child we can observe this phenomenon. Many of the experiences we value most greatly in life involve the sharing and interconnection of personal data. It is no exaggeration to say that some of the most meaningful events in our lives necessarily entail the interconnection of our personal data with the personal data of others. For example, marriage, the joint purchase of a house, entering a business partnership, and executing a will or trust, are all potentially life-changing events through which the interactions between two (or possibly more) people will shape and alter the personal data of all those involved.

It is not, however, just a case of individuals being affected by the processing of the personal data of those they interact with, but of how the processing of an individual's nominally personal data as part of a larger group can affect the personal data of people completely unrelated to the individual themselves. There are a number of situations in which this is increasingly becoming the case, particularly in the context of big data analytics. As noted by Mantelero:

"...the use of big data analytics creates "a new truth regime", in which general strategies are adopted on a large scale on the basis of representations of society generated by algorithms, which predict future collective behaviour. These strategies are then applied to specific individuals, given the fact that they are part of one of more groups generated by analytics."<sup>65</sup>

Mantelero goes on to note how "PredPol", a type of software used by US police forces to anticipate and prevent criminal offences, is a notable example of this phenomenon. PredPol, and other similar software, operates by cross checking data relating to types and locations of recent crimes and how they were committed. These analyses allow for predictions to be made regarding how and when future crimes will be committed.<sup>66</sup> However, this can also induce a "self-fulfilling cycle of bias". If the software predicts that many crimes are likely to be committed in a particular area police forces will allocate more resources to those areas. This will increase the number of crimes detected in those areas, thereby reinforcing the original prediction. Concurrently, a reduced police presence elsewhere may reduce crime detection in other areas and generate an adverse prediction. This may bring about the undesirable consequence of geographical discrimination, which may not directly affect any one individual, but may severely impact on entire communities and everyone living in them in terms of social stigma.<sup>67</sup>

This approach to data processing is also used by health insurance companies, which extract predictive information about the risks associated with groups of clients based on their television viewing, purchase habits, ethnicity, and location.<sup>68</sup> In such cases, predictions based on correlations identified following such analyses do not only affect individuals who act differently from the rest of the group, but may affect all persons within that group and set that group aside from the rest of society. Neighbourhood general credit scores (i.e., the practice adopted by credit companies to provide specific opportunities to people living in a specific location in a way that bears no connection to their living conditions but is based on aggregate analyses of group data) is a good example of this phenomenon.<sup>69</sup>

In these sorts of situations (i.e., where the processing of one individual's personal data may have effects on other individuals or groups of individuals completely unrelated to the individual themselves) the consent, and to some extent even the preferences, of the individual effectively become extraneous. Consider the following scenario:

There are one hundred people living in a neighbourhood. Twenty of these people consent to their personal data being processed by a credit company for the purposes of credit

<sup>65</sup> A Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' [2016] 32(2) Computer Law & Security Review 238-255.

<sup>66</sup> PredPol advertises itself as a predictive policing company that attempts to predict crimes based on the use of predictive analytics. See: PredPol, (PredPol – The Predictive Policing Company) <https://predpol.com/> accessed 10 April 2021.

<sup>67</sup> A Mantelero (n 78).

<sup>68</sup> *Ibid.*

<sup>69</sup> *Ibid.*

scoring. The credit company then processes the personal data of these twenty people for credit scoring purposes. The remaining eighty people do not consent to any involvement in this exercise, and their personal data are not processed. The credit company then analyses the data provided by a minority of the entire population (i.e., the twenty consenting individuals) to determine the range of what can be inferred for the majority (i.e., the entire one hundred person population, including the eighty non-consenting individuals). Based on the preceding analyses, the credit company predicts that all residents of the neighbour are likely to be a high credit risk, and the entire credit score of everyone living in the neighbourhood (including the eighty non-consenting individuals) is lowered.

In this scenario the eighty non-consenting individuals have been adversely affected by analyses of the personal data of the twenty consenting individuals.<sup>70</sup> The fact that the eighty non-consenting individuals have not given consent, or have perhaps withheld consent, has made no difference to how they are treated. Concurrently, the consent of the twenty consenting individuals has effectively allowed for their interests to ride roughshod over the interests of the eighty non-consenting individuals. Barocas and Nissenbaum refer to this phenomenon as “tyranny of the minority”: a choice forced upon the majority by a minority with whom they have no meaningful or recognised relations.<sup>71</sup> In so doing, the scenario demonstrates how in situations where our personal data are interconnected with the personal data of others, and processed in ways that can affect others, the value and of a one individual’s consent is significantly diminished.

The above examples of the interconnectedness of our nominally personal data with the data of others shows us that to some extent such data are “personal” in name only. Such data will often either be inextricably linked to other persons, and it is only through a consideration of their relationship with these other persons that the full meaning of those data can be derived. Concurrently, the processing of “our” data is capable of having significant (possibly negative) effects on others. With this being the case the notion that individuals should be presumed to enjoy a default entitlement to control such data in all contexts is questionable. Similarly, the notion that individual consent should either be required for, or sufficient to legitimise, all uses of such data is similarly dubious.

<sup>70</sup> Research has highlighted, for instance, that multiple attributes pertaining to entire groups of people can be inferred when as few as 20% of the groups members reveal their attribute information. See: A Mislove et al, ‘You are who you know: inferring user profiles in online social networks’ [2010] WSDM ’10: Proceedings of the third ACM international conference on Web search and data mining 251-260. See also: A Vedder, ‘KDD: the Challenge to Individualism’ [1999] 1(4) Ethics and Information Technology 275-281.

<sup>71</sup> On this issue, see: S Barocas and H Nissenbaum, *Big Data’s End Run around Anonymity and Consent*. in J Lane et al (eds), *Privacy, Big Data and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 63. See also: R Alunge, “‘I am Datafied Because We are Datafied’: an Ubuntu Perspective on (Relational) Privacy [2020] 33 Philosophy & Technology 595-612.

### 5.1.2. Data mutability

Our personal data are constantly changing. Personal data, like any other kind of information, are subject to change, misrepresentation, distortion, or may simply be inaccurate.<sup>72</sup> However, despite widespread acknowledgement of personal data’s malleable nature, this nuance is arguably still insufficiently appreciated. Our personal data not only constantly contribute to the world we live in but are contributed to by it. By the time a person dies, many, if not most, of their personal data will be drastically different from the point at which they were born. Data pertaining to a person’s health, religious beliefs, political affiliations, sexuality, employment, appearance, and contact details can change considerably at different points of a person’s life as they grow and/or interact with external environments.

Some of these changes will be voluntary and fall within the scope of the individual’s control. For instance, a person may voluntarily choose to move home (e.g., they may decide, as a matter of personal preference, they would like to relocate from an urban area to a rural area). This would inevitably necessitate a change in the person’s personal data (e.g., their location data, contact details etc.). However, many changes to a person’s personal data that will occur over the course of their life will not be controllable or even predictable. As a result, we must recognise that individuals only have limited control over the shape, condition, and state of their personal data. A person’s body, for instance, may succumb to illness, obesity, or pain, thereby necessitating an involuntary change to their medical data. A person may have to move home due to being evicted by their landlord, or due to a natural disaster making their home uninhabitable, thereby necessitating an involuntary change to their location and contact details. A person may adjust their appearance to conform to conditions of employment set by their employer. A person’s religious and political views may be significantly influenced by ideas and materials they are exposed to on online platforms, with said platforms themselves determining which material gets shown to users algorithmically based on analyses of the personal data of other users.<sup>73</sup>

What this mutability of nominally personal data once again shows is that to some extent such data are “personal” in name only. The condition and status of an individual’s personal data will inevitably be heavily influenced by external (i.e., non-personal) factors. In other words, a person’s personal data will literally be the product of their interactions with their external environment, many of which will be entirely involuntary. With this being the case, suggestions that individuals should have control or sovereignty over such data, or that individual interests should supersede the interests others who are also part of the external environment which determine the condition and status of those data, are questionable. This will likely particularly be the case for communitarian ethicists, who deny that people can be defined by focusing on characteristics of lone individuals, and maintain that they can only be

<sup>72</sup> P Birkinshaw, *Freedom of Information: The Law, the Practice, and the Ideal* (Cambridge: Cambridge University Press 2010).

<sup>73</sup> L Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (London: Free Press 2013) 34.

defined by reference to their environing community.<sup>74</sup> Some communitarian scholars have argued, for instance, that if a person's ontology is derived from the existence of the community, and the individual's participation in the community, the individual does not and cannot exist alone. Accordingly, the individual owes their personhood, identity and existence to their community, and thus it is morally incumbent on the individual to act in a way that prioritises supporting and giving back to that community.<sup>75</sup> Pursuant to this, if personal data are a reflection of the individual's personhood and identity, and such data are themselves similarly shaped by interactions within the community, the logical extension of the general communitarian position would be that we should prioritise uses of those data that are for the betterment of the community. A necessary corollary of this position would be a diminution of the ability of individuals to restrict, authorise, or otherwise control uses of such data (e.g., requiring consent of the individual for PMDD uses of their medical data).

### 5.1.3. Discussion

According to the communitarian school of thought there are at least two compelling reasons for why we should at the very least think about the possibility of moving away from the traditional vision of personal data (i.e., that personal data are data that concern only ourselves, and that individuals should automatically be presumed to have a default sovereignty over such data). It is instead arguable that we should recognise that to a significant degree the state and condition of our personal data depend heavily on external conditions, contextual peculiarities of our lives, and interconnections with the personal data of others, and that in some contexts the handling and usage of data that are nominally "ours" can significantly affect others.

None of the arguments presented above deny that personal data comprise an essential part of our identities. Whilst our personal data, including medical data, will inevitably be shaped by external conditions, context, and interconnections, they still provide a representation to others of the people we are. They are data that can identify us, determine how we are treated by others, and determine our role in society. In a real sense, then, our personal data are not just ours, but a part of us. The arguments presented above, however, whilst accepting this general premise, stress the idea that a necessary and inevitable feature of our personal data is that they contribute to, and draw from, the world around us as well as the personal data of others. Whilst personal data represent us and are a part of us, they are in no way exclusively our own, and we should recognise that in some situations others may have a legitimate interests in uses of data that are nominally "ours". With this being the case, the communitarian position holds that the collection and retention of medical data as part of PMDD initiatives should not be regarded as being in any way unusual, and thus it should not require any unusual degree of consent from any involved parties before the law permits it.

<sup>74</sup> See, for example: A Menkiti, *Person and community in African traditional thought*. in R Wright (ed), *African philosophy: An introduction* (University Press of America 1984) 171.

<sup>75</sup> A Mbiti, *African religions and philosophies* (Anchor Books 1970) 141.

Instead, PMDD should be considered as part of a natural interaction between the personal data of a person and the personal data of others in the person's environment, which commences at birth and continues beyond death.

Accordingly, a communitarian approach to PMDD might hold that the law should start by treating it as a reflection of the natural, and inevitable, interactions that occur within a community of individuals, and the interdependence and interconnection of data that is "personal" only nominally. The rationale for this position would be that as all of us have participated in, and benefited from, such interactions during our lives, there is arguably a presumption that this is something we would wish to continue to be involved in after we die, and thus the law should not indulge any notion that suggests personal data are simply one's own. With this being the case, communitarian observers might argue the influence of the individual and their consent in any PMDD regulatory framework should be kept to a minimum, or perhaps not included at all.

## 5.2. Broader ethical arguments

In addition to the above-mentioned communitarian arguments that may be invoked in opposition to consent being required as part of any PMDD regulatory framework, another complimentary strand of arguments contend, regardless of whatever communal character nominally personal data may have, the idea that consent should be required for the storage and use of medical data post-mortem is at best unjustifiably self-indulgent, and at worst morally indefensible. These are collectively referred to as broader ethical arguments.<sup>76</sup>

### 5.2.1. The incoherency of "posthumous consent" and "posthumous rights"

The first argument considered here relates to the possible conceptual incoherency of the notion of posthumous consent (i.e., the idea that an action performed on a person who is deceased will only be ethically and legally legitimate if consent was given by that person whilst they were still alive). The crux of this argument is that consent, as set out above, is intended to protect the autonomy of living individuals and to protect such individuals from harm, not to indulge the wishes deceased persons, ergo, consent is ill-equipped and inappropriate for deployment in matters relating to PMDD.

A useful starting point for considering this argument is to recall the centrality of the role of the individual (i.e., the "data subject") in European and UK data protection law. The central role played by the individual in the European and UK data protection frameworks is a function of the importance they afford to autonomy and self-determination. This can be seen in several ways. Notably, as alluded to above, the consent of the data subject is one of the six legitimising grounds set out in the GDPR and UK GDPR through which the processing of personal can be rendered lawful. Chapter 3 of the GDPR and UK GDPR also set out a range of rights to which all data subjects are entitled in respect of their personal data. The rationale for

<sup>76</sup> The arguments made here are largely inspired by those made in relation to organ donation by John Harris. See, particularly: J Harris, 'Law and regulation of retained organs: the ethical issues' [2006] 22(4) *Legal Studies* 527-549.

the inclusion of these provisions is a desire to give the individual the ability to exert control and influence over their personal data, and an ability to determine when, how, why, and by whom those data are used.

As is the case in other areas of law, the GDPR and UK GDPR utilise consent as a tool for legitimising acts that would otherwise amount to a wrongdoing, and for giving effect to individual autonomy. For instance, in situations where processing personal data would otherwise be unlawful, the consent of the data subject is generally sufficient to render that processing lawful. However, in the absence of any other legitimising ground for personal data applying in such a situation the processing of the personal data of a person who has not consented will not only be unlawful, it will also be a denial of the ethic of respect for that person. As noted by Harris:

“Respect for persons is widely regarded as the fundamental basis of any ethics involving human beings. It is an assumption of our society and indeed most, if not all, others that it is persons that have the highest moral importance or value. There may be differences over how to define a person and difficulties about when persons begin and cease to exist, but the ultimate value of those deemed to be persons is largely unchallenged... Respect for persons, then, not only describes the outcome – treating others in morally appropriate ways, but also points to the origin of this obligation in the ultimate supreme moral value of individuals of a particular sort.”<sup>77</sup>

Harris goes on to note how respect for persons has two distinct dimensions: 1) respect for autonomy, and 2) concern for welfare.<sup>78</sup> The role of consent, and other rights within EU and UK data protection law largely reflects this position. The adoption of consent-based values in the GDPR and UK GDPR, for example, is based on 1) respect for the wishes of the data subject; and 2) ensuring that personal data are used for legitimate and ethical purposes in line with the wishes of the person to whom they relate.<sup>79</sup> From this we can identify how it might be argued that consent-based values should be adopted by, and play a central role in, the regulation of PMDD. As noted above, for instance, proponents of post-mortem privacy have argued that the same justifications for allowing control over personal data in life apply equally to control of personal data post-mortem, and ergo that consent should be required for medical data of deceased persons to be collected and used as part of PMDD initiatives. However, for several reasons, the idea the law should allow post-mortem control over personal data in the PMDD context is contestable.

It is well known that various areas of law recognise that individuals can have enduring interests that survive death. The laws of wills and probate, and equity and trusts, for example, allow individuals to make testamentary dispositions in respect of their tangible and intangible property. The arguments set out here in no way challenge the validity of this notion. They accept that individuals can have posthumous interests, and that there is nothing automatically egregious about the law protecting such interests. However, there are notable

arguments that interests of this sort can, and must, be distinguished from the types of interests that consent as a concept is intended to protect, including those relating to matters of data protection and PMDD.

As highlighted above, consent is a mechanism that is designed to protect and give effect to an individual's autonomy, and to legitimise actions done to that individual that, in the absence of consent or other justification, would otherwise be illegitimate. Pursuant to this, the problems with suggestions that consent should play a prominent role in the regulation of PMDD become immediately apparent. Autonomy, by definition, requires an individual to have the capacity to make choices regarding their preferences, options, and decisions.<sup>80</sup> Deceased persons, however, have no capacities at all. A person who is no longer alive has no free will, no preferences, nor do they have any desires, wants, or even needs. Consequently, the autonomy of deceased persons is incapable of being violated because a deceased person has no autonomy to violate.<sup>81</sup> Their autonomy has extinguished upon death. Ergo, if consent is a mechanism for protecting autonomy, in the context of PMDD it is incapable of performing its ordinary intended function. Deceased persons simply have no need for consent as it is a mechanism designed to protect a value that they do not possess. Accordingly, the notion that it should be required for their medical data to be incorporated into PMDD initiatives, therefore, arguably represents nothing more than an unjustified and conceptually incoherent indulgence of individual preferences.

The question then becomes “but what about wishes made during life?”. If the wishes of a deceased person that were made clear at a time the person was still alive were not respected, would this amount to a breach or frustration of their autonomy? As established above, just as some individuals have preferences in respect of what happens to their bodies after death, some will have preferences about what happens to their personal data. It arguably holds to reason, therefore, that if these preferences are not respected, their autonomy may have been posthumously violated. This position, however, is again likely to be highly contentious. Consider the following scenario:

When Person A was a young child, the parents of Person A uploaded pictures of Person A to a popular social networking platform and registered an account in the name of Person A. As an adult, Person A wishes that this had not been done, and objects to the data-handling practices of the social networking platform.

Did the fact that Person A's personal data were processed in this way by others, before Person A was autonomous and had formed a view on such matters, frustrate Person A's autonomy because Person A now wishes this had not occurred? Some observers would argue that no violation of autonomy has occurred. Harris, for instance, argues that a person hav-

<sup>80</sup> In addition to the scholarly considerations of autonomy set out above, this approach to autonomy has also been endorsed by UK courts. See, for example, the judgment of Lord Donaldson in *Re T (Adult)* [1992] 4 All ER 649.

<sup>81</sup> J Harris (n 89). See also: Winter, S. (2010). Against posthumous rights. *Journal of Applied Philosophy*, 27(2), 186–199.

<sup>77</sup> *Ibid.*, 529.

<sup>78</sup> *Ibid.*

<sup>79</sup> See: E Kosta (n 26).

ing autonomous wishes at one point in time about something that happened at a previous point in time when they were not autonomous does not equate to their autonomy being frustrated or violated. This, he contends, would only occur if an autonomous preference that was expressed at the time an individual was autonomous was frustrated.<sup>82</sup> According to this logic, in the example given above the actions of Person A's parents whilst Person A was a child are clearly contra to the wishes Person A holds as an adult, but it no way has Person A's autonomy been violated. By the same token, just as decisions taken regarding Person A's personal data *before* Person A was autonomous cannot be said to violate Person A's autonomy, neither can decisions taken regarding Person A's personal data when Person A is *no longer* autonomous (e.g., once Person A has died).

But what about the rights of the dead more generally? Should individuals not have rights to determine what happens to their medical data post-death regardless of any autonomy-related implications (or the absence thereof)? As set out above, there are various arguments that may be invoked in support of this general position. As others have contended, however, it is doubtful whether there is any such thing as a posthumous right. For instance, in his seminal book, *The Morality of Freedom*, Joseph Raz suggests that an individual can possess rights if, and only if, their wellbeing is of ultimate importance.<sup>83</sup> If we are to accept this premise then it holds to reason that dead persons can have no rights, as they have no wellbeing for the simple reason that they have no "being" at all. They are not beings, but ex-beings.<sup>84</sup> Whilst there may well be some situations in which individuals can have interests that will survive their death, and these interests may be deserving of legal protection, it is important to note that the impact, or "harm", that may be experienced because of a posthumous wish not being respected or upheld will be qualitatively different to that which would usually be experienced in the event of the interests of wishes of a living person not being respected. For instance, criminal offences that may be committed against the body of a deceased person (e.g., performing a sexual act on a corpse)<sup>85</sup> do not involve violations of autonomy in the same way an offence committed against the body of a living person might (e.g., rape or battery). By the same token, improper and illegitimate uses of a deceased person's personal data are unlikely to result in any harm in the same way as would be the case were said person still alive. A useful illustrative example of is again provided by Harris:

<sup>82</sup> *Ibid.*

<sup>83</sup> J Raz (n 24).

<sup>84</sup> J Harris (n 89) 534. See also: J Taylor, *Death, Posthumous Harm, and Bioethics* (Abingdon: Routledge 2012). It is also worth noting that in its jurisprudence the European Court of Human Rights has repeatedly stated that the rights set out in the European Convention on Human Rights (ECHR) apply only to living persons. See: *Jäggi v. Switzerland*, App. No. 58757/00, 47 Eur. H.R. Rep. 30 (2006); *Estate of Kresten Filtenborg Mortensen v. Denmark*, App. No. 1338/03, 2006-V Eur. Ct. H.R. (2006); *Koch v. Germany*, App. No. 497/09, Eur. Ct. H.R. (2012).

<sup>85</sup> In England and Wales, Section 70(1) of the Sexual Offences Act 2003 establishes that a person will be guilty of a criminal offence if they intentionally perform an act of sexual penetration on a body part of a dead person.

"...if I have an interest during my life that my children are provided for after my death and I see to secure that interest by executing a will, it remains true that if the provisions of that will are not respected, my interests have been harmed, although of course neither will I be aware of that fact, nor will it affect my well-being in any way..."<sup>86</sup>

In the context of PMDD initiatives, we might sketch the following analogous situation:

"...if a person expresses an interest during their life that their medical data are not stored and used for the purposes of medical research after their death, and their wishes are not respected, their interests will have been harmed, although of course neither will they be aware of that fact, nor will it affect their well-being in any way."

The crux of the point being made here is that in the context of PMDD legal rights and rules relating to consent and control of personal data are simply incapable of performing their normal function of giving effect to individual autonomy and protecting individuals from harm, and thus they lack any coherent conceptual justification for inclusion in the regulation of PMDD. The reason for this is simple: deceased persons have no need for legal mechanisms that give effect to their autonomy as they have no autonomy at all, and have no need for legal rights designed to protect them from harm as they are incapable of being harmed.

5.2.2. *The strength of communal/societal needs and interests*  
The absence of any harms or impact to a person's wellbeing notwithstanding, there are, as noted above, prima facie compelling arguments that can be made in respect of why interests and wishes pertaining to retaining post-mortem control of personal data should be respected in many, if not most, contexts. Nevertheless, PMDD is an example of an area of application that arguably should be excluded from this general ethos. This is because though there may well be prima facie compelling reasons for respecting an individual's wishes in respect of posthumous uses of their medical data generally, it is arguable that in the context of PMDD these interests are relatively weak when compared to the interests of individuals who may benefit from future uses of those data. In other words, though deceased individuals may have interests regarding future uses of their medical data, these interests are outweighed by those of individuals who are still alive. To this end, it might be suggested that the issue of whether the wishes of deceased persons regarding their medical data should be respected should be determined by the same principle which is generally used to determine whether the wishes of a deceased person regarding the disposal of their assets and their estate should be respected. That is to say, such wishes should be respected subject to competing public interests. This is usually the case, for example, with wills and other testamentary dispositions, where the wishes of deceased persons are normally respected subject to the public interest of death duties being paid in the form of taxes and similar.<sup>87</sup> This is in stark contrast to the interests of living persons, who due

<sup>86</sup> J Harris (n 89).

<sup>87</sup> *Ibid.*

to the possibility of suffering immediate physical and emotional harms if their wishes are not respected, have a much stronger claim to their interests being upheld.

However, even if a failure to uphold the wishes of the deceased in respect of future uses of their medical data do not affect the deceased themselves, there are two main ways in which their wishes are “person affecting” in the PMDD context. First, they are person-affecting in the sense that they may affect individuals who would potentially benefit from the results of research undertaken on the medical data of the deceased. Second, the use of such data may affect any persons who would be distressed by, or would otherwise object to, the data being collected, retained, or used. For instance, if the medical data of the deceased were to be used for illicit purposes (e.g., to perpetuate an act of fraud) or to form the basis of decisions about people still alive, the rights or interests of friends or relatives of the deceased, or perhaps of other individuals might be engaged. For instance, as noted above, data pertaining to the DNA or genome of the deceased could contain information about their family members, and these family members could conceivably have legitimate concerns about how future uses of such data could have implications for their own genetic privacy. The family or friends of the deceased may also have conscientious beliefs which may also be engaged by the practice of PMDD. Alternatively, in the absence of any such beliefs, they might simply possess a strong desire that the wishes of the deceased in relation to their medical data are respected, perhaps due to believing this is fitting or appropriate. We have seen already that all these factors might give rise to arguments that the consent of affected individuals should be required if medical data are to be extracted and retained as part of any PMDD initiative. For instance, if Person A correctly believes that analysis of their medical data may compromise the genetic privacy of Person B, a failure to respect Person A’s wishes may result in Person B being harmed. Requiring Person A’s consent prior to their medical data being utilised as part of any PMDD initiative could possibly prevent this harm from occurring. In the absence of the consent of the deceased themselves, it might even be suggested that consent decisions should pass to friends and family of the deceased. However, for various reasons this should arguably not be the case.

As a general matter, there is of course nothing *prima facie* wrong with treating the powerful feelings of friends and family members of the deceased in respect of the deceased’s medical data with courtesy and respect. In the context of PMDD it must be remembered, however, that these are not the only interests at stake, and thus it should not necessarily be assumed that they should automatically be given priority. Instead, it would perhaps be preferable for these interests to be balanced against the powerful feelings or interests of others who desire the medical data of deceased persons to be available for scientific, research and therapeutic purposes. There is no obvious reason, for instance, why the needs and interests of the family and friends of the deceased, no matter how compelling, should *de facto* triumph over the needs and interests of other people and families to not to be unnecessarily bereaved for want of medical data that could be used to research and develop medical treatments for their sick relatives.

In many other areas of law, such as Human Rights, conflicts of interests or values are resolved by analyses of which carry the most moral weight. In other words, by an analysis of whether the interests served by one set of values outweigh the importance of another. For example, Article 8(1) of the European Convention on Human Rights bestows on all individuals the right to a private and family life. Article 8(2) then specifies how public authorities may legitimately interfere with individuals’ enjoyment of this right if doing so is necessary to carry out activities in which there is an overriding public interest, such as protecting national security or ensuring freedom of expression. There is no discernible reason why any legal or regulatory framework pertaining to PMDD should be any different. To this end, there numerous possible justifications for the idea that in the PMDD context the interests of the wider community should prevail over those of deceased persons. The most significant of these reasons is the fact that the interests of the wider community, the members of which will still be alive, protect an interest in life itself. Medical data collected from deceased persons, and subsequently used as part of a PMDD initiative may, as established previously, be capable of making substantial contributions to the development of medical treatments that could quite literally be life-saving. None of the counterpoised interests considered above (i.e., the interests of the deceased, family members, or other individuals, in medical data not being collected and utilised for PMDD purposes) protect such an urgent value. As mentioned above, this is not to say that the interests of the deceased and other individuals are not deserving of respect, they are simply demonstrably weaker than the demands with which they are in competition.

As already established, the collection, retention and use of the personal data of deceased persons as part of PMDD initiatives serves numerous valuable purposes. The investigation and analysis of such data has the potential to be hugely beneficial to a vast number of people (e.g., individuals whose lives may be saved by cures developed pursuant of PMDD-related research). In this regard, it is possible to draw comparisons between PMDD initiatives and biobanks, which are now widely recognised as being of critical importance in terms of their contribution to research, diagnoses, treatments, and care within healthcare systems worldwide.<sup>88</sup> It is no exaggeration to say that many of the techniques, treatments, and therapies available through modern medicine from which we all benefit have in no small part been made possible because of retained tissues and organs.<sup>89</sup> As outlined above, PMDD initiatives have

<sup>88</sup> A Cambon-Thomsen, ‘Assessing the impact of biobanks’ [2003] 34 *Nature Genetics* 25-26; JE Olson et al, ‘Biobanks and personalized medicine’ [2014] 86(1) *Clinical Genetics* 50-55; L Andrews, ‘Harnessing the Benefits of Biobanks’ [2005] 33(1) *The Journal of Law, Medicine & Ethics* 22-30; J Kinkorová, ‘Biobanks in the era of personalized medicine: objectives, challenges, and innovation’ [2016] 7 *EPMA Journal*.

<sup>89</sup> J Harris (n 70) 543. Economic analyses have also suggested that organ donation saves the UK National Health Service (NHS) hundreds of millions of pounds annually. See: S Madden et al, ‘The effect of consent rates for deceased organ donation in Wales after the introduction of an opt-out system’ [2020] 75(9) *Anaesthesia* 1146-1152.

the potential to make similar contributions to the advancement of medical science. As with organ donation, each denied donation of medical data (e.g., through a refusal to give consent) could have significant negative cumulative knock-on effects for research into future treatments and therapies.<sup>90</sup> To this end, it is no exaggeration to say we all have an immense interest in the collection of medical data of deceased persons, and in such data being made readily available for research purposes. A necessary implication of this position, therefore, is that not only are the strengths and justifications of the interests of deceased persons regarding future uses of their medical data generally weaker than those of persons who are alive, but that in the context of PMDD the wishes of the deceased in respect of their medical data have no moral basis on which to claim precedence over the interests and needs of the living.<sup>91</sup>

Against this background, the purpose of comparing PMDD initiatives to biobanks is to highlight that refusal to contribute to PMDD initiatives would arguably be deeply selfish and immoral. The implications of this are twofold. The first is that any suggestion that the idea the law should require opt-in consent for the retention of deceased persons' medical data as part of PMDD initiatives is in any way consistent with public or personal morality is manifestly false. The second is that in situations where the views of the deceased are not known, there should be a *de facto* presumption that they *would* have wished to contribute to, or at least not impede, the development of a vital resource that has the potential to save many lives (i.e., PMDD initiatives).

### 5.3. Discussion

The crux of the arguments presented in this section is twofold. First, in the context of PMDD, the opt-in ante-mortem consent of deceased persons would arguably be incapable of performing the normal role of consent in protecting autonomy, bodily integrity, or well-being. In the best-case scenario, we might therefore say respect for consent in the PMDD context would be more like extending a courtesy than respecting a right. In the worst-case scenario, we might say that were the law to require opt-in ante-mortem consent for the medical data of deceased persons to be incorporated into PMDD initiatives this would amount to nothing more than an incoherent, unethical, and unjustifiable attempt to indulge individual preferences in the face of competing collective interests that have greater moral authority. Second, whichever of these interpretations one favours, it is categorical that we all benefit from the social practice of medical research (i.e., the primary purpose of

PMDD initiatives). Were it not for the development of medical treatments and therapies, such as antibiotics and vaccines, many of us would not be here today. Most of us will continue to benefit from these advances throughout the course of our lifetimes, and thus we arguably have a moral obligation to contribute to, or at least not to impede, the social practices which produce them, and ergo our opt-in consent should not be a condition of our participation.

## 6. The way forward

The previous sections of the paper set out multiple arguments for and against the idea that the opt-in consent of the individual, expressed ante-mortem, should be required for the medical data of deceased persons to be lawfully incorporated into PMDD initiatives. We are now left with several questions: Where do we go from here? Should opt-in consent be required? Would it be appropriate the law not to require opt-in consent? If opt-in consent is not required as a general matter, should consent be removed from the equation entirely?

One possible option for the regulation of PMDD, and perhaps the simplest, would be conscription. In other words, the law should grant medical practitioners the automatic authority to retain and utilise the medical data of the deceased as part of PMDD initiatives without requiring any authorisation. Various observers have advocated for the adoption of this sort of approach in the context of regulating organ donation. Spital and Taylor, for example, argue that any sort of consent requirement for the recovery of transplantable organs should be eliminated from any legal or regulatory frameworks relating to the extraction and retention of human tissue, equating this to a situation of total war in which most people would accept the concept of a military draft as being in the public interest.<sup>92</sup> Were such an approach to be deployed in the PMDD context medical data of deceased persons would essentially *de facto* become medical property. Retention where no beneficial use could be made of the data, or retention for purposes unrelated to PMDD, could be outlawed as a means of protecting the interests of the deceased and/or their relatives. For the reasons set out above, there are *prima facie* compelling reasons as to why conscription of the use of medical data of deceased persons for PMDD-related purposes could be viewed as morally and ethically justifiable. A regulatory approach in this vein would perhaps offer coherence and consistency. However, it would also fundamentally alter the character of PMDD from a notion primarily associated with the "donation" of one's medical data, to one better described as involving such data being "taken". This would be undesirable, as it could lead to PMDD being schematised as what some have termed a "Cartesian extraction of a useable resource",<sup>93</sup> rather than the altruistic and philanthropic endeavour it undoubtedly is. Another pos-

<sup>90</sup> On the impact of legal rules that allow the veto of organ donations, see: KA Bramstedt, 'Family refusals of registered consents: the disruption of organ donation by double-standard surrogate decision-making' [2013] 43(2) Internal Medicine Journal 120-123; J Wilkinson (n 31); A Spital and JS Taylor, 'Routine recovery of cadaveric organs for transplantation: consistent, fair, and life-saving' [2007] 2(2) Clinical Journal of the American Society of Nephrology 300-303.

<sup>91</sup> For an argument as to why we all have a moral duty to contribute to organ donation schemes, see: PT Menzel, 'The moral duty to contribute and its implications for organ procurement policy' [1992] 24(5) Transplant Proc. 2175-2178.

<sup>92</sup> A Spital and JS Taylor, 'Routine recovery of cadaveric organs for transplantation: consistent, fair and life-saving' [2007] 2(2) Clinical Journal of the American Society of Nephrology 300-303.

<sup>93</sup> D Leder, *Whose Body? What Body?* in M Cherry (ed.) *Persons and their Bodies: Rights, Responsibilities, Relationships* (Dordrecht: Springer 1999) 260.

sible option would be propertisation, under which individuals would formally be granted proprietary rights in their medical data, thereby allowing them to sell those data to the operators of PMDD initiatives. As noted elsewhere, however, an approach in this vein would also be plagued by huge, and likely insurmountable, ethical and practical difficulties.<sup>94</sup>

In spite all that has been said above in terms of both how in the context of PMDD consent is arguably incapable of performing its normal role, or how, given the interests and needs of living persons in the wider community, there is no ethical justification for allowing deceased persons to restrict posthumous uses of their medical data, it might still be suggested that as a general matter consent, or at least some form of authorisation, is always preferable to conscription. This will even usually be the case where neither consent nor authorisation are required by law. As alluded to by Brownsword and Goodwin, for instance, in any regulatory system it is preferable, for the sake of preserving whatever sense of moral community we might have, that individuals are given the choice to voluntarily do the “right” thing for the right reasons, rather than the law forcing them to behave a certain way. In their words, it is the capacity of human beings to decide for themselves what their priorities are, to rank those preferences, to reason, and to choose for themselves what their lives should be, which makes human beings “special”.<sup>95</sup> To put this another way, respect for these values is a prerequisite for the boundary-marking concept of human dignity. To act in ways that traverse this boundary would place the action and actor outside the bounds of humanity, which would be a “very dangerous place to be”.<sup>96</sup> To this end, any PMDD regulatory regime that ordained to completely remove any element of individual choice regarding post-mortem uses of medical data would arguably represent an unjustifiable affront to human dignity.

At this point, it is important to recall that none of the anti-consent arguments established in the preceding section were intended to challenge the notion that people may, for a variety of reasons, have perfectly valid interests in how their personal data are used by others. The arguments set out here merely served to highlight how although individuals may have interests in what happens to their medical data post-mortem, these interests should not be mischaracterised as entailing any sort of inviolable sovereignty in terms of determining posthumous uses of such data, and that in most circumstances these interests will be weaker than other competing

interests in those data. Pursuant to this, even if the law did not require opt-in ante-mortem consent, it may still be possible to find a regulatory solution which respects the interests of those on both sides of the consent debate.

One prima facie plausible way of ensuring the above-mentioned competing interests were given the respect they deserve would be by adopting a presumed consent model of PMDD regulation. Under this approach, all adult persons would automatically be presumed to consent to their medical data being retained and utilised for PMDD purposes post-mortem unless they had made it known that they did not wish for this to occur. In other words, each person would be given a right to object to, or “opt-out” of, PMDD initiatives.<sup>97</sup> A person’s objection could be based on their faith, culture, or beliefs, and would be respected in the face of everything other than the strongest competing interests.<sup>98</sup> The value of medical data to PMDD initiatives would therefore be prioritised whilst, concurrently, individuals would still be given a choice regarding whether they wanted to become a “donor”, thereby preserving their autonomy. In such a system, objections could be routinely recorded in health records, or perhaps another form of PMDD register, and could be accessed when needed.<sup>99</sup>

Critics of this approach may contend that a failure to object would not amount to an expression of the deceased’s wishes in any meaningful way, and thus would not meaningfully give effect to their preferences. However, in response to this it could be argued that within a society where levels of willingness to engage with public health initiatives are expected to be high,<sup>100</sup> the approach proposed here is likely to reflect the preferences of deceased persons to donate more accurately, or at least no less accurately, than under a system of opt-in consent.<sup>101</sup> It might logically be assumed, for instance, that individuals who were opposed to their medical data being used for PMDD purposes would be more likely to opt-out under a system of presumed consent, than individuals who

<sup>94</sup> H Pearce (n 70); P Hummel, M Braun and P Dabrock, ‘Own Data? Ethical Reflections on Data Ownership’ [2020] *Philosophy & Technology*. For an overview of an analogous debate regarding whether the law should grant proprietary interests in their organs, see: R Nwabueze, ‘Donated organs, property rights and the remedial quagmire’ [2008] *Medical Law Review*.

<sup>95</sup> R Brownsword and M Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge: Cambridge University Press 2012) 191.

<sup>96</sup> *Ibid.* Other observers have advanced similar perspectives. Grayling, for instance, suggests that if people are prevented from arriving at our own choices, conclusions, and aims on their own, they will never be capable of any worthwhile moral or social development. AC Grayling (n 24) 263-265.

<sup>97</sup> Some observers, for instance, have argued there are compelling ethical reasons as to why silence (i.e., a failure to register an objection) should be taken to equate to a positively expressed consent in some medical contexts. See: B Saunders, ‘Opt-out organ donation without presumptions’ [2012] 38(2) *Journal of Medical Ethics* 69-72.

<sup>98</sup> Section 7 of the UK Human Tissue Act 2004 specifies that the storage and use of bodily material without consent will be lawful if this would be in the public interest. A similar principle could be incorporated into an opt-out consent for regulating PMDD.

<sup>99</sup> In the United Kingdom, the NHS currently operates a secure database (The NHS Organ Donor Register) that keeps records of all organ donations decisions. There is no obvious reason why a similar database could not be established for PMDD purposes.

<sup>100</sup> For instance, figures recently published by NHS Blood and Transplant (NHSBT) showed that in 2019/2020 there was an observable marked increase in public support for organ donation. See: NHS, *Organ Donation and Transplantation Activity Report 2019/2020*. Available at: <https://www.organdonation.nhs.uk/helping-you-to-decide/about-organ-donation/statistics-about-organ-donation/transplant-activity-report/>.

<sup>101</sup> D Price, ‘Legal framework governing deceased organ donation in the UK’ [2012] 108(1) *British Journal of Anaesthesia* 68-72; C Cohen, ‘The case for presumed consent to transplant human organs after death’ [1992] 24(5) *Transplant Proc.* 2168-2172.



desired to donate would be to opt-in under an opt-in consent system. This assumption stems from the fact that most individuals who were opposed to their medical data being used for PMDD purposes would likely have conspicuous religious or moral beliefs underpinning their objections, of which they themselves would be very much aware, and would therefore be unlikely to neglect to opt-out of a system of presumed consent.<sup>102</sup> Empirical research has also demonstrated that, worldwide, the adoption of opt-out models of consent have generally improved increased levels of organ donations and transplants, and have helped to prevent shortages.<sup>103</sup> It seems plausible, therefore, that they could have a similarly beneficial effect for PMDD initiatives were they incorporated into relevant regulatory structures.

Though some might argue that an opt-out approach would imply that our medical data effectively belong to the state as soon as we die, and that it would amount to nothing more than an attempt to give a so-called 'eminent domain' policy a cloak of respectability, so to make it acceptable to a society that places a high value in individual rights, this would not be the case.<sup>104</sup> As established above, it is not simply a question of whether our medical data either do, or should, belong exclusively to ourselves, the state, or to any other party, but one of recognising that whilst we all have interests in data about us, there is no moral justification for thinking that our own interests should always de facto prevail over the interests of others. Even observers with the strongest commitment to individualist ethics would, for instance, surely accept that individual sovereignty over medical data cannot be treated as an absolute or inviolable notion, and that to some extent a balance must be struck with communitarian interests, even if there were disagreements regarding exactly how and where this balance should be struck.<sup>105</sup> For these reasons, a presumption of consent would ethically and morally defensible in the context of retaining and utilising the medical data of de-

ceased persons for PMDD purposes, so long as information on the opt-out approach proposed above was made readily available ante-mortem and provided in a comprehensible format.

## 7. Conclusion

As is evident from the contrasting views considered throughout this paper, finding an appropriate legal response to questions pertaining to the role of the individual in any PMDD regulatory framework will be hugely challenging. The optimum solution would be the construction of a regulatory framework and of legal principles that simultaneously promote health-care, medical research, and the development of new treatments and therapies whilst respecting and taking account of people's preferences concerning the retention and utilisation of medical data of deceased persons. It is, however, perhaps unlikely that any single approach or regulatory model would be capable of addressing all the nuances inherent in the competing arguments set out above.

The argument tentatively made here is that there are *prima facie* compelling reasons why the law should not require the opt-in ante-mortem consent of deceased persons for the lawful retention and utilisation of their medical data post-mortem for PMDD purposes. However, considering the possible competing interests at stake, the law should provide individuals with a right of refusal, or to object, to their medical data being used posthumously for these purposes. This right should not be absolute, and its exercise should be considered in light of any competing interests. In the absence of any objection being expressed, the law should presume a willingness to medical data being used for PMDD purposes.

It is likely that this solution would be considered too lenient by some, and perhaps overly strict by others. Concurrently, however, it can just as easily be argued that the opt-out/right to object approach suggested here would achieve, to some extent at least, overlapping consensus between the abovementioned competing moral views. It is an approach that would simultaneously recognise the valuable contribution the medical data of deceased persons can make to medical research and treatments, and that medical data, and the treatment thereof, is fundamentally connected to respect for a person's dignity. To this end, the approach proposed here is the product of the deliberative analysis and consideration of the strongest competing views, and one which would minimise the differences between them. This would clearly not be enough to guarantee the favour of all persons on either side of the consent debate, but as its use would be supported by defensible logic and reasoning, hopefully most reasonable observers would consider it to be legitimate.

Regardless of whatever regulatory solution for PMDD is adopted, however, there are various issues touched upon in this paper which would benefit from further research and analysis. One interesting question is, regardless of whether the law is to adopt opt-in or opt-out approach to consent in the context of PMDD, what should happen in situations where a person lacks capacity to make an informed decision? One suggestion might be that decision-making authority should pass to next of kin, or another family member of relative. This, how-

<sup>102</sup> MB Gill, 'Presumed consent, autonomy and organ donation' [2004] *Journal of Medical Philosophy* 29(1) 37-59.

<sup>103</sup> See, for example: M Ahmad et al, 'A Systematic Review of Opt-out Versus Opt-in Consent on Deceased Organ Donation and Transplantation (2006-2016)' [2019] 43 *World Journal of Surgery* 3161-3171; A Albertsen, 'Deemed consent: assessing the new opt-out approach to organ procurement in Wales' [2018] 44(5) *Journal of Medical Ethics* 314-318; S Madden et al, 'The effect on consent rates for deceased organ donation in Wales after the introduction of an opt-out system' [2020] 75(9) *Anaesthesia* 1146-1152;

<sup>104</sup> The term 'eminent domain policy' is generally used to refer to policies which treat private property or other private commodities as something that is automatically usable by the state for the pursuing a goal that is supposedly in the public interest. For a discussion of eminent domain policies in the context of organ donation, see: RM Veatch and JB Pitt, 'The myth of presumed consent: ethical problems in new organ procurement strategies' [1995] 27(2) *Transplantation Proceedings* 1888-1892.

<sup>105</sup> On the issue of reductions in individual informational self-determination being counterbalanced by the facilitation of public and independent authorities acting in the interests of society, see: A Mantelero, 'The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' [2014] 30(6) *Computer Law & Security Review* 643-660.

ever, would further complicate the issues considered throughout this paper. Closely related to this are questions regarding what ante-mortem support could or should be put in place to help people to make informed decisions regarding posthumous uses of their medical data, and what would be required for these to work effectively in practice. Further research regarding religious and cultural attitudes to posthumous uses

of personal data, and the implications they may have for regulating PMDD, would also likely be useful.

---

### **Declaration of Competing Interest**

There are no conflicts of interest to report.