

Your data will never die, but you will: A comparative analysis of US and UK post-mortem data donation frameworks

Dr Edina Harbinja, Aston University and Henry Pearce, University of Portsmouth

Abstract

Posthumous medical data donation (PMDD) for the purpose of legitimate, non-commercial and, potentially, very beneficial medical research has been sparsely discussed in legal scholarship to date. Conversely, quite an extensive social science and humanities research establishes benefits of this practice. It also finds that PMDD enables individuals to employ their altruistic motivations and aspirations by helping them participate in ‘citizen’s science’ and medical research, thus supporting efforts in finding cures for some of the acutest diseases of today.

There appears to be no jurisdiction where a regulatory framework supports and enables PMDD. This paper analyses whether and to what extent law and policy should enable this practice. We take a comparative approach, examining the position under both US and UK law, providing the first comparative legal account of this practice.

We do not aim to suggest a detailed legal solution for PMDD, but rather key considerations and principles for legislative/policy reforms, which would support the practice of PMDD. We discuss organ donation and provide a comparative outlook with the aim of drawing lessons from this practice, and applying them to the regulation of PMDD. Our analysis is both normative and black letter since we consider arguments regarding the necessity of organ and data donation, as well as the law that regulates these practices.

1. Introduction

Individuals are not able to donate their medical data posthumously for the purpose of legitimate, non-commercial and, potentially, very beneficial medical research. There appears to be no jurisdiction where a regulatory framework, or indeed the law, supports and enables this philanthropic cause. Whilst some policy options for donation under limited circumstances and for limited purposes exist, there are no practices through which a person can proactively donate their medical data or patient records for a specific research purpose, or more generally, for any non-commercial or commercial medical research with a worthwhile cause, in a way comparable to organ donation. This paper analyses whether and to what extent law and policy should enable posthumous medical data donation (hereinafter: PMDD). We take a comparative approach, examining the position under both US and UK law, providing the first comparative legal account of this practice. We focus exclusively on the post-mortem donation of one’s patient records for medical research purposes, and not the donation all of their personal data, although occasionally for illustrative purposes we refer to a wider variety of data.

Researchers in social science and humanities have discussed PMDD extensively. This practice enables individuals to employ their altruistic motivations and aspirations by helping them participate in

'citizen's science' and medical research.¹ Krutzinna et. al. put forward ten key persuasive arguments for PMDD, including solidarity, altruism, the right to science, but also economic and other social and ethical reasons.² Benefits of PMDD include supporting advanced and personalised medical research, and providing a basis for data mining, machine learning and AI, thereby helping to generate new understandings of some of the most severe medical concerns facing humanity (e.g. cancer and mental illness).³ In the US, researchers have found that the deceased subject Integrated Data Repository (dsIDR) at Marshfield Clinic will contain more deceased patients than living patients by 2056.⁴ Their confirmatory assessment at IDR of Columbia University Medical Center in New York showed a similar trend.⁵ This is a significant amount of data that will have considerable value, even in the context of a fragmented health care system, such as that of the US. In the UK, NHS records are more centralised. In England, for instance, this is achieved through the Spine platform, which is also used for the data opt-out regime, discussed below.⁶

Legal scholarship in the area is extremely sparse. One of the first papers in the field, however, was written by Harbinja as a part of her work towards The Code for Posthumous Medical Data Donation, developed by the Digital Ethics Lab at the Oxford Internet Institute.⁷ Harbinja's paper focused on UK law and regulation, or rather, the lack of it. The paper explored how health data and medical records are currently protected in the UK, with a particular focus on the medical data and records of the deceased. She also examined other key issues around ownership and succession of personal data for the purpose of establishing their effects on PMDD. The paper briefly considered some overarching parallels with organ donation legislation to determine whether there are lessons to be learned from this comparable area of law. The conclusion drawn from the abovementioned analyses was that a bespoke regulative regime for PMDD is needed. This, ideally, would require making amendments to the General Data Protection Regulation to ensure harmonisation and consistency across the EU, as well as between general and sector-specific data protection laws and policies. Another option she considered was the introduction of an NHS policy that would govern PMDD, similar to the current NHS option that allows individuals to opt-out of their data being used for medical research.⁸ In another salient paper, Sorbie argues that consent of the deceased should not be a 'silver bullet' for such a regime and that there is room for setting up a more balanced framework. The author proposes a dynamic data governance framework, consisting of institutions that control data flows and can issue

¹ Vayena E, Tasioulas J. (2015) "We the Scientists": a Human Right to Citizen Science'. *Philosophy & Technology*. 28: 479–485; Krutzinna J., Taddeo M., Floridi L. (2019)" Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data". in: Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer, Cham

² Krutzinna, Taddeo and Floridi, ibid.

³ Prainsack, B. (2014) "The Powers of Participatory Medicine". *PLoS Biology*. 12(4): e1001837; Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series.

⁴ dsIDR initially started as a research idea for a local or a central repository of the deceased's health records in the USA, or its parts. The repository facilitates researchers' access to valuable data without fulfilling all the conditions required for the use of the data of the living individuals, as per HIPAA. For more see: Huser V. and Cimino J.J. (2013) "Don't take your EHR to heaven, donate it to science: legal and research policies for EHR post mortem" *AMIA Jt Summits Transl Sci Proc*, 95. eCollection, at:

<https://www.ncbi.nlm.nih.gov/pubmed/24303243>

⁵ Huser, Vojtech & Miller, Aaron & K Vawdrey, David. (2014) "Evaluating the size of deceased patient EHR research data sets: A multi-year trend analysis" 10.13140/2.1.4229.0884.

⁶ NHS Digital, Systems and services, "Spine", at <https://digital.nhs.uk/services/spine>

⁷ Krutzinna, Taddeo and Floridi (n 1)

⁸ Harbinja E. (2019) "Posthumous Medical Data Donation: The Case for a Legal Framework" in: Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer, Cham, p. 102.

authorisation for the use of medical records in public interest (such as the Confidentiality Advisory Group (CAG) in England and the Public Benefit and Privacy Panel (PBPP) in Scotland; we discuss the role of CAG in the following section).⁹

This paper builds on the abovementioned research and offers the first comparative analysis of UK and US legal and regulatory frameworks regarding PMDD. The paper's purpose is not to suggest a detailed legal solution for PMDD, but rather key considerations and principles for legislative/policy reforms, which would enable the practice of PMDD. We discuss organ donation in much greater depth in this paper and provide a comparative outlook with the aim of drawing lessons from this practice, and applying them to the regulation of PMDD. Our analysis is both normative and black letter since we consider arguments regarding the necessity of organ and data donation, as well as the law that regulates these practices. In section 2, we discuss post-mortem legal protection of the deceased's data and patients records in the UK and US. We examine the current law and policies in the UK and US to establish which regime is more suitable for PMDD and whether, if any, constituent mechanisms could be incorporated into a PMDD regulatory framework. Section 3 then analyses organ donation regulatory regimes in the UK (England primarily) and the US (at a federal level). The purpose of this section is to identify similarities and potential regulatory solutions that we could apply to a future PMDD regulatory regime. Finally, we offer suggestions for a regulatory framework for PMDD.

2. Legal protection of the deceased's health data and patient records in the UK and US

Harbinja discusses the legal protection of the deceased's' health data in her earlier paper, but the analysis is limited to the EU and UK. For clarity, we briefly set out these findings here before making comparisons with US law and policy. We expand on her earlier analysis of certain points, particularly those concerning the NHS opt-out regime for using data beyond direct care purposes.

2.1. UK law and policy

The EU data protection framework does not protect the deceased's personal data. This is made clear by Recital 27 of GDPR, which explicitly excludes the personal data of deceased person's from its scope. The recital does, however, allow the Member States to expand their national data protection regimes to include such data if they wish. The UK has opted not to take this approach, with s. 3(2) DPA 2018 defining personal data as information relating to 'living individuals' only. This means that health data and patient records of deceased persons, which would ordinarily be special category data,¹⁰ are not protected at the EU or UK level. Accordingly, the processing (i.e. almost any use) of the personal data of deceased persons does not need to comply with the data protection principles, nor does it require a legitimising ground.¹¹

⁹ Sorbie A. (2019) "Medical Data Donation, Consent and the Public Interest After Death: A Gateway to Posthumous Data Use" in: Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer, Cham

¹⁰ Health-related data in the EU and the UK belong to 'special categories of personal data' (article 9 General Data Protection Regulation 2016 (GDPR) and s. 10 and 11 of the Data Protection Act 2018 (DPA 2018)). Processing of the special categories of data is in principle prohibited by the GDPR, and only allowed on the basis of ten general grounds, including relevant grounds for health data, as per art. 9 2. (a), (c), (h), (i), (j) GDPR and schedule 2 part 6 of the DPA 2018.

¹¹ See: Arts 5 and 9 GDPR.

Nevertheless, in the UK, the lack of general data protection of the deceased's medical data has been somewhat mitigated by sector-specific legislation. For example, the Access to Health Records Act 1990 states that health records must be kept securely and that access is only permitted in limited circumstances.¹² In England, GP health records are passed on to Primary Care Support England and retained for 10 years after death. This period can be extended for up to 100 years. Additionally, The Public Records Act 1958 stipulates that GP records will become public when forwarded to local authorities after the death of the patient. Most records are closed for 30 years post-mortem and those related to physical and mental health are closed for 100 years. Permission can be sought from the Public Records Office to use data of deceased persons in research if confidentiality can be guaranteed.¹³ The Department of Health advises that hospital records are kept for 8 years. Interestingly, however, at the policy level, there is already a regime for the use of data of the deceased. The NHS, for instance, has recently extended their data opt-out regime for purposes beyond direct care, including research, to include the data of the deceased, with an option for a pre-mortem opt-out.¹⁴ This means that records will be used in research *inter alia*, unless there is a wish to the contrary expressed by the deceased.¹⁵ Researchers can submit requests for the use of confidential patient information which will be considered by the Confidentiality Advisory Group (CAG). Interestingly, the data opt-out regime does not apply where a person has given their explicit consent to other specific uses of their medical data.¹⁶ The NHS bases this principle on a recommendation of the Caldicott Review, i.e. 'People should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care. This should apply to patients' decisions made both before and after the implementation of the new opt-out model'.¹⁷ Noticeably, the NHS does not specify if this exemption applies to the deceased's data and their pre-mortem consent for the use of their data for specific purposes. It could be argued that, due to the general application of the policy to the deceased's data,¹⁸ this would be the case. Consequently, this would mean that nothing in this policy prevents an individual from opting for PMDD.

Common law also provides some protection for the deceased's medical data. There is some suggestion, for instance, that the common law duty of confidence, which doctors owe to their patients, might survive the death of the patient.¹⁹ The issue is unsettled in the law, as indicated by Harbinja.²⁰ For the purpose of this paper, however, we argue there is sufficient evidence to claim that

¹² See, for instance, section 3(1)(f) of the Act, which allows for a personal representatives of the deceased, or individuals with claim arising out of the death of the deceased, to access the deceased's medical records.

¹³ Medical Research Council (2003) "Ethics Series: Personal Information in Medical Research"

<https://mrc.ukri.org/documents/pdf/personal-information-in-medical-research/> and Harbinja (n 8) pp. 101 – 103.

¹⁴ NHS (2019) "National Data Opt-out Operational Policy Guidance Document", 4 March 2019, at:

<https://digital.nhs.uk/services/national-data-opt-out-programme/operational-policy-guidance-document>

¹⁵ Ibid, s. 6.

¹⁶ Ibid.

¹⁷ National Data Guardian for Health and Care (2016) "Review of Data Security, Consent and Opt-Outs" June 2016, at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF, s. 3.2.30.

¹⁸ 'A national data opt-out continues to be maintained and applied for an individual after they have died. Health and adult social care organisations are expected to continue to apply opt-outs for deceased patients and their opt-out will continue to be held on the Spine repository.' NHS (n 14), s. 2.

¹⁹ *Lewis v Secretary of State for Health & Anor* [2008] LS Law Med 559; Decisions by the Information tribunal support this stance (see *Webber v IC and Nottinghamshire Healthcare NHS Trust* GIA/4090/2012 and *M v IC and Medicines and Health Products Regulatory Authority* GIA/3017/2010)

²⁰ Harbinja (n 8), p. 201.

the duty of confidence does survive the death of the patient. There is, of course, a need to clarify this area of law and we hope that case law will develop in a way that affirms of a post-mortem duty of confidence. It is important to note here that the National Health Service Act 2006 allows the Secretary of State for Health and Social Care to make regulations to authorise or mandate the processing of confidential patient information (CPI) for specific medical purposes and, thus, to set aside the common law duty of confidence. The regulations made under this provision are the Health Service (Control of Patient Information) Regulations 2002 (SI 2002/ 1438) ('COPI Regulations'). They enable the disclosure of CPI without consent as long as the requirements of the regulations are met and the person responsible for the information complies with all other relevant legal obligations including those imposed by data protection legislation. Relevant purposes include those relating to patients referred for the diagnosis or treatment of cancer to be processed for the medical purposes (Regulation 2), and the diagnosis, control, prevention or recognition of communicable diseases and other risks to public health (Regulation 3). Regulation 5 provides an avenue for CPI to be processed for medical purposes set out in the Regulation's Schedule, including 'the audit, monitoring and analysing of the provision made by the health service for patient care and treatment'. Applications for access under Regulation 2 or 5 are submitted to CAG who provide independent expert advice to the relevant decision-maker (Health Research Authority for research applications and the Secretary of State for non-research applications).²¹ A standard condition of CAG's advice seems to be that patient objections to the use of this information should be respected. Notably, CAG has stated it will not be in the public interest to override an objection 'in anything other than the most exceptional circumstances'.²² An implication of this is that, in effect, patient's consent or its withdrawal through an opt-out regime, such as that described above, would maintain the duty of confidence and prevent the use of CPI for research purposes defined by Regulations 2 and 5. It is unclear whether this applies to deceased CPI. The significance of consent and opt-out in this process demonstrates the need for PMDD, and for a clear mechanism through which consent can be obtained regarding CPI being used for research purposes.

2.2. US law and policy

US law generally does not protect personal data of the deceased.²³ At the federal level, researchers are encouraged to share data by the America COMPETES Act.²⁴ This law relates to data already used by researchers, rather than enabling access to the medical records of deceased individuals that have not previously been the subject of research. Ethical approval by an institutional review board (IRB) is required for every research activity intended for publication. For general, non-research uses of electronic health record (EHR) data, a change in January 2013 to the HIPAA privacy rule (aka 'the omnibus rule') shortened the protection of personal health information (PHI) from an indefinite period of time to a period of 50 years from the patient's death. This is considered a period of protection that extends over two generations, similar to that used in the context of copyright.²⁵ The HIPAA permits state law to extend this provision, meaning states are not pre-empted by the federal requirements. For example, the state of Hawaii still mandates indefinite protection.²⁶ Given what we have said about

²¹ Regulations 2002 (SI 2002/ 1438), Regulation 5.

²² NHS Health Research Authority, (2018) "National data opt-out" 24 May 2018, at:

<https://www.hra.nhs.uk/about-us/news-updates/national-data-opt-out/>

²³ Edwards, L. and Harbinja, E. (2013) "Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World" *Cardozo Arts & Entertainment Law Journal*. 32(1): 83-129; Harbinja, E. (2017). "Post-mortem privacy 2.0: theory, law, and technology" *International Review of Law, Computers & Technology*, 31(1): 26-42. doi:10.1080/13600869.2017.1275116

²⁴ America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science Act, 20 USC 9801

²⁵ Kels, C. G. et al. (2013) "Medical Privacy After Death: Implications of New Modifications to the Health Insurance Portability and Accountability Act Privacy Rule" Mayo Clinic Proceedings, Volume 88, Issue 10, 1051 – 1055, p. 1051.

²⁶ Haw. Rev. Stat. section 323C-43

the protection of health records and patient data in the UK, US protection generally seems to last for a longer period of time.

The HIPAA, however, allows for the disclosure of PHI of decedents without IRB or privacy board approval.²⁷ Such disclosures are dependent on three conditions: (1) use is sought solely for research on the PHI of decedents; (2) the researcher can provide, on request, documentation of the death for subjects used in the study; and (3) the PHI is necessary for the research - the 'decedent research clause'. Interestingly, some institutions interpret this rule as requiring researchers to obtain authorisation from next of kin, or a waiver of authorization from an IRB or Privacy Board, in order to access the PHI of decedents.²⁸ This is a very restrictive interpretation of the HIPAA provision. However, perhaps understandably, research ethics processes often include additional non-legal requirements to mitigate ethical risks that are not of a legal nature.²⁹ The likely reason for this is the effect research might have on the next of kin and relatives of the deceased, for instance, the revealing of hereditary diseases.

In summary, US law protects the deceased's patient records for at least 50 years post-mortem. Researchers are allowed to access such data for research purposes if they fulfil the three requirements set out above. However, as ethical processes require additional authorisations this is not a common occurrence. After 50 years PHI can generally be freely used in research unless a state has a provision to the contrary (see the example of Hawaii). Difficulties may arise, however, in relation to the availability of PHI, and how such data are stored, maintained and deleted. Given the fragmented nature of the US health care and associated systems, this could constitute a barrier to access to such data for researchers after legal protection has expired, especially in the lack of repositories such as the dsIDR mentioned in section 1.

In terms of doctor and patient confidentiality, state case law sets out different rules as to whether and to what extent the duty survives the patient's death.³⁰ For example, New Jersey courts have hinted that physicians might have to balance their duty to warn relatives at risk of hereditary diseases with their duty of patient confidentiality.³¹ Statutes also offer varied legislative approaches. Some state laws uphold the confidentiality of genetic information, and other states limit confidentiality with certain exceptions.³² Oregon legislation, for instance, permits the disclosure of genetic data when it is pertinent to medical diagnoses of relatives of the deceased.³³ The American Medical Association Code of Ethics clearly states that doctors have the obligation to protect patient information, including information obtained post mortem.³⁴ There are exceptions to this rule, including, *inter alia*, a patient's explicit consent or directive. In spite of disparate state law, therefore, confidentiality does generally seem to extend beyond the patient's death. Similar to the UK, this has been achieved through policies, occasionally statutes, and, to a lesser extent, by case law.

²⁷ HIPAA - protected health information (PHI) 45 CFR 164.512(i)(1)(iii)

²⁸ Ness R. (2007) "Influence on the HIPAA Privacy Rule on health research" *JAMA*, 298(18): 2164–2170.

²⁹ Research ethics codes and procedures thus include values that may underpin the law, but are not necessarily legal categories, e.g. honesty, objectivity, openness, competence etc.

³⁰ Berg, Jessica Wilen, (2001) "Grave Secrets: Ethical and Legal Analysis of Postmortem Confidentiality" Faculty Publications. 572.

https://scholarlycommons.law.case.edu/faculty_publications/572

³¹ *Safer v Estate of Pack*, 677 A2d 1188 (NJ Supp 1996).

³² King M. (2000) "Physician duty to warn a patient's offspring of hereditary genetic defects: balancing the patient's right to confidentiality against the family member's right to know—can or should Tarasoff apply?" *Quinnipiac Health Law J.*; 4(1):1-38.

³³ Disclosure of genetic information; exceptions. Or Rev Stat section 192.539 (2011).

³⁴ AMA, "Code of Medical Ethics overview", at: <https://www.ama-assn.org/delivering-care/ethics/code-medical-ethics-overview>

2.3. Comparison

A comparison of UK and US regimes reveals that neither requires consent for the processing of the deceased's health data. At a sector-specific level, however, the American system seems clearer and more permissive in respect of using data for medical research, with some discrepancies at the state level. The UK Access to Health Records Act 1990, for instance, makes no provisions for researchers to access patient records. The NHS Act 2006, Regulations of the Secretary of State for Health, and NHS policy allow for the granting of access in limited circumstances, in the absence of any patient wish to the contrary. The US is more permissive at the legislative level, but less so at the policy level, since ethical procedures require consent from the next of kin, or waiver of this authorisation by an appropriate institution. The upshot of this, therefore, is that policy and legislative interventions in both countries would be necessary if a PMDD regulatory regime was to be introduced, and for its framework to be coherently set out. Even in the more permissive environment of the US, there is no option for a person to actively opt-in to PMDD. Researchers can access such data under the conditions considered above, but this has nothing to do with the deceased's wishes or consent. UK policy, on the other hand, mentions consent but does not establish a mechanism through which it can be recorded and executed. The NHS data opt-out policy in the UK is the closest thing to what could be considered a form of PMDD. However, this is an opt-out regime and is not specific enough in terms of purpose and benefits so to qualify as PMDD. In addition, the fact that it can be overridden by a specific consent prevents it from being what we consider to be true PMDD.

3. Organ donation and data protection: closely aligned rationales

Having discussed the potentially applicable law and policy to PMDD, and argued that fresh regulatory interventions are required, we now consider the law of organ donation. In this section and the next, we outline and compare UK and US regimes, and identify some important challenges inherent in the construction of any PMDD regulatory framework.

The purpose of organ donation legislation is to regulate the post-mortem handling of bodily material. The majority of developed nations worldwide have bespoke organ donation laws and, though approaches differ, most examples of such legislative frameworks have two core objectives. The first: to establish and protect individual autonomy and posthumous bodily integrity. The second: to facilitate important and innovative uses of bodily material, notably for medical research or transplantation. A primary example of such a piece of legislation is the UK Human Tissue Act 2004,³⁵ passed following scandals at the Bristol Royal Infirmary and Royal Liverpool Children's Hospital in 1999-2000, the details of which were revealed by the Kennedy and Redfern Inquiries.³⁶ The Act, as considered in more detail below, contains a number of provisions that enshrine the right of individuals to control what happens to their bodily material post-death. Against this background, organ donation laws represent a useful starting point for discussions regarding the construction of a regulatory framework for PMDD.³⁷ The most significant indicator of this is the fact that organ donation laws, such as the HTA, and data protection laws, such as the GDPR and DPA 2018, are rooted in the similar theoretical ground, and share an analogous rationale as well as various conceptual and practical

³⁵ [hereinafter HTA 2004]

³⁶ For an overview of the details of these scandals, see: Sheach Leith, V. (2007) "Consent and nothing but consent? The organ retention scandal", *Sociology of Health & Illness*. See also: Burton, J. and Underwood, J. (2003) "Necropsy practice after the "organ retention scandal": requests, performance, and tissue retention", *Journal of Clinical Pathology*.

³⁷ [hereinafter PMDD]

similarities.³⁸ If we look at the key concepts central to both organ donation laws and data protection laws, and how they are treated, this is immediately apparent.

As alluded to above, organ donation laws are ordinarily concerned with regulating the handling of “bodily material”, or similar, to prevent such material being used for unethical or inappropriate purposes. Data protection law, on the other hand, is concerned with regulating the processing (i.e. almost any use) of personal data, and ensuring that any processing complies with the data protection principles.³⁹ Immediately we see a similarity. Both types of legislation identify a central concept around which their entire operation is based and subject the treatment, handling, and use of that concept to various rules. If an action does not pertain to the said concept the substantive rules of the legislation will not be engaged. Any action not involving “bodily material”, for instance, will generally fall outside the scope of organ donation laws. Likewise, the processing of any non-personal (e.g. anonymous) data will fall outside the scope of data protection law.⁴⁰ This is an initially superficial comparison. If we look more closely at these two concepts, however, it is evident that this similarity goes much deeper. Specifically, the notions of bodily material and personal data are themselves conceptually alike, and the need to regulate their usage and/or handling is frequently justified by way of reference to a comparable rationale.

Bodily material and the need to control its handling by legal means is most frequently justified by way of reference to the identity of the individual to whom it relates. To this end, organ donation laws identify bodily material as an innate aspect of a person’s personhood and express its protection in the form of legal values. The crux of this position is that legal rules of this sort are critical to the protection of autonomy, bodily integrity, and human dignity.⁴¹ Data protection law operates on a similar basis. The recitals of the GDPR, for instance, specify how the processing of personal data must be consistent with values and notions intrinsically linked to individual personhood and dignity, such as the right to a private and family life.⁴² The implication of this is that personal data themselves comprise of a fundamental aspect of an individual’s personhood. This position has been endorsed in the academic and scholarly literature, with some observers opining that personal data, like bodily material, are an extension of the self, and must be treated with the same respect as the physical person to whom they relate.⁴³ Weight has been added to such assertions by empirical research that has demonstrated how the analysis of certain types of personal data can be deeply revealing of aspects of an individual’s identity.⁴⁴ The upshot of this, therefore, is that both organ donation laws and data protection law are

³⁸ It should perhaps be noted, however, that whilst data protection rules in the USA do not formally recognise proprietary interests in personal data, but academic calls for the introduction of such are widely thought to originate from the US. See e.g. Westin, A.F. (1967) *Privacy and freedom*, New York. Atheneum; Laudon, K.C. (1996) “Markets and privacy” 39 (9) *Communications of the ACM* 92-104, at 96; Schwartz, P.M. (2003) “Property, privacy, and personal data” 117 *Harvard Law Review* 2056-2128; Mell, P. (1996) “Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness” 11 *Berkeley Technology Law Journal* 1-79.

³⁹ See: Article 5 GDPR.

⁴⁰ See: Recital 26 GDPR.

⁴¹ Evans, R., & E. Ferguson. 2014. Defining and measuring blood donor altruism: a theoretical approach from biology, economics and psychology. *Vox sanguinis*. 106(2): 118-126 and Price, D. 2000. *Legal and Ethical Aspects of Organ Transplantation*. Cambridge: Cambridge University Press

⁴² Recital 4 GDPR.

⁴³ See, for instance: Stevenson, S. quoted in *Ethical Technology Use, Policy and Reactions in Educational Settings*, ed. by Beycioglu, K. (2012) Hershey, PA: IGI Global. Pg.87. See also: Microsoft (last accessed December 2017) “Personal Control of Data”, <https://www.microsoft.com/en-us/research/video/personal-control-of-data/>

⁴⁴ For instance, a 2013 study by the National Academy of Sciences of the United States of America demonstrated that a wide variety of an individual’s personal attributes, ranging from their sexual orientation

prima facie concerned with providing individuals with protection in respect of a commodity, or concept, which is directly and inextricably linked to their personhood. In other words, both aim to protect something that is “personal” to the individual (whether bodily material or data), and justify the pursuit of this aim by way of reference to unacceptable threats to personhood and human dignity that would manifest in the absence of regulatory intervention.⁴⁵ As explored below, both areas of law seek to achieve this objective by providing individuals with means through which they can exercise control.

A further similarity regarding the legal treatment of bodily material and personal data is that, whilst their respective legislative regimes outline rules and rights that allow individuals to exercise control over a commodity intrinsically linked to their personhood, neither couch such provisions in the language pertaining to the protection of proprietary interests. Ordinarily, negative rights pertaining to restricting the access to, or use of, commodities are recognised as property rights, and formally denoted as such.⁴⁶ This, however, is generally not the case for rules of this type found in legislation pertaining to organ donation and data protection. Using the HTA 2004 as an example once again, some have argued that its rules regarding negative control over bodily material only make sense if we accept individuals have proprietary interests in their body parts,⁴⁷ but this is surely incorrect. As considered below, and convincingly argued elsewhere, the rights contained within the HTA protect autonomy and dignity-related interests and do not formally recognise the existence of property rights in the human body.⁴⁸ Similar observations can be made in respect of data protection law’s treatment of personal data. Though the desirability and existence of property rights in personal data is a topic that remains hotly contested, the orthodox view is that despite some aspects of data protection law evincing “property-like” features, individuals do not formally enjoy property rights in their personal data.⁴⁹ The rights enshrined in legislation pertaining to organ donation and data protection, therefore, both prima

to intelligence, can be automatically inferred from personal data taken from social networking sites such as Facebook. Kosinski, M. Stillwell, D. and Graepel, T. (2013) “Private traits and attributes are predictable from digital records of human behaviour”, *Proceedings of the National Academy of Sciences of the United States of America*. pg.4.

⁴⁵ On this issue, see: Pearce, H. (2018) “Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?”, *Information and Communications Technology Law* 27(2), pp.133-165; Harbinja (n 23); Floridi, L. (2016). “On human dignity as a foundation for the right to privacy” *Philosophy and Technology*. doi: 10.1007/s13347-016-022.

⁴⁶ See: L Becker, *The Moral Basis of Property Rights*. in R Pennock and J Chapman (eds), *Nomos XXII: Property* (New York University Press 1980) 187-220; P Eleftheriadis, ‘The Analysis of Property Rights’ [1996] 16(1) Oxford Journal of Legal Studies 31-54; J Penner, *The Idea of Property in Law* (Oxford University Press 1997) 71; S Balganesh, ‘Demystifying the Right to Exclude: Of Property, Inviolability, and Automatic Injunctions’ [2008] 31(2) Harvard Journal of Law & Public Policy 593; T Merrill, ‘Property and the Right to Exclude’ [1998] 77(4) Nebraska Law Review 730

⁴⁷ See, for example: Price, D. (2009) *Human Tissue in Transplantation and Research: A Model Legal and Ethical Donation Framework*, Cambridge: Cambridge University Press; Pattinson, S. (2011) “Directed donation and ownership of human organs”, *Legal Studies*. See also: Nwabueze, R. (2008) “Donated organs, property rights, and the remedial quagmire”, *Medical Law Review*.

⁴⁸ Herring, J. and Chau, P.-L. (2007) “My body, your body, our bodies”, *Medical Law Review*; Herring, J. (2016) *Medical Law and Ethics*, Oxford: Oxford University Press. Also of note is the way in which US courts have traditionally recognised quasi-property rights, if not full property rights, in dead bodies and corpses. On this issue, see: Zee, J. (2008) “The Revised Uniform Anatomical Gift Act: Bringing California Donation up to Contemporary Medical, Legal and Bioethical Practices”, *McGeorge Law Review*.

⁴⁹ See: Pearce, H. (2018) “Personality, property and other provocations: exploring the conceptual muddle of data protection rights under EU law”, *European Data Protection Law Review* 4(2); E Harbinja, ‘Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could be the Potential Alternatives?’ [2013] 10(1) SCRIPTed 26; Harbinja (n 23); Lyskey, O. (2014) “Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order”, *International Comparative Law Quarterly* 63(3).

facie treat personhood-related commodities as aspects of an individual's personality rather than property.

Closely related to the second similarity is the way the rights granted by organ donation and data protection rules regarding individual control are not absolute. Both types of legislation recognise the value of bodily material and personal data as commodities and the need for wider communal interests to triumph over those of the individual in some situations. Article 17 of the GDPR, for instance, confers on individuals the controversial "right to be forgotten", which allows them to acquire erasure of their personal data from data controllers. This right, however, is not absolute and attempts to exercise it may not always prevail against other competing interests.⁵⁰ Similar observations can be made in respect of rules often found in organ donation legislation. As is considered in more detail below, for instance, the HTA's rules relating to individual control of bodily material will not apply in a range of exceptional situations. The upshot of this is that whilst both areas of law attempt to give individuals sovereignty in respect of a commodity central to their personhood, this sovereignty is far from absolute. Both areas of law, therefore, are premised on the belief that whilst individuals should enjoy autonomy in respect of personhood-related commodities, individual interests must occasionally cede to those of the community.

4. Organ donation legislation in practice

For the reasons stated above, organ donation legislation represents a logical and sensible starting point for discussions regarding how to construct a legal framework for PMDD. The next step in our analysis is to examine precisely how organ donation laws operate in practice, and whether any lessons can be derived from their experiences. To do this we use two prominent legislative regimes as case studies: the UK Human Tissue Act 2004, referred to above, and the US Uniform Anatomical Gift Act 2006.

4.1. The UK Human Tissue Act 2004

Section 1 of the HTA specifies it will be lawful to remove, store, or use "human material"⁵¹ from deceased and living persons provided "necessary consent" has been obtained, and the removal,

⁵⁰ This is made explicitly clear by Art.6(1)(g) GDPR where it is stated specified that the processing of personal data will be lawful when it is "necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject". Art.6(1)(g), therefore, implies that a balancing exercise which weighs the legitimate interests of the data controller against the rights of data subjects if personal data processing activities are to be legitimised on the basis of the data controller's legitimate interests. This is an issue that has been considered by both the Article 29 Working Party and, more recently, the CJEU. See: Article 29 Working Party (2014) Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217 and Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, EU:C:2017:336. More generally, EU data protection law also allows for the rights and interests of individual data subjects to be balanced against other competing interests, such as national security imperatives. On this issue, see: A Dimitrova and M Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy Makers after the NSA Affair' [2017] 54(3) Journal of Common Market Studies 636

⁵¹ "Human material" is defined by section 53 HTA as including the tissue, cells and organs of human beings, but excluding hair, nails, and gametes and embryos stored outside of the body.

storage, or use is done for a purpose listed in schedule 1 of the Act. Consent, however, is not defined by the Act itself, and is instead explained by the Human Tissue Authority Code of Practice on Consent:⁵²

“For consent to be valid it must be given voluntarily, by an appropriately informed person who has the capacity to agree to the activity in question.”⁵³

It is further specified that consents must be expressed positively (i.e. “opt-in”), and that a failure to object, or acquiescence, will not be sufficient.⁵⁴ Moreover, consents must be specific, relate to a particular purpose, and can be withdrawn at any time.⁵⁵ If consent is not obtained, the removal, storage, or use of bodily material will, as a general matter, be a criminal offence.⁵⁶ This rule applies regardless of whether the person from whom material is extracted is alive or deceased. In other words, the removal of material from a corpse will require consent if it is to be lawful.

Interestingly, however, the HTA allows for consent to be given by an individual other than whom from which the human material is to be extracted. Though section 3 specifies that in circumstances involving living adults consent must be obtained from the adult himself or herself, assuming they have the capacity to give consent,⁵⁷ different rules apply in situations involving deceased persons. According to the HTA, consent to extract material from a deceased individual can be obtained one of three ways. First, the deceased themselves can give consent via a will or other testamentary disposition. Second, assuming the deceased did not declare their intentions prior to death, an appointed representative, appointed by the deceased prior to death, can give consent on the deceased’s behalf. Third, if no representative has been appointed, the person in the closest “qualifying relationship” can give consent.⁵⁸

From this overview we the value and significance the HTA places upon consent is clear. Its utilisation in the manner outlined above (i.e. a de facto presumption that no extraction of bodily material is allowed unless consent is present) shows precisely how the HTA gives the individual considerable sovereignty in respect of their bodily material and its usage, even post-death. Whilst this is the default position, however, there are numerous exceptions. For example, under section 7 of the Act, when consent has not been given, the Human Tissue Authority has the power to deem (i.e. infer) its existence. This power can be used when it is impossible to trace the individual from whom material originates, or in situations where reasonable attempts have been made to obtain consent but no response has been received. High Court Orders can also be used to mandate the removal of human material from the body of a person, living or dead, without consent, if this is deemed to be in the public interest.⁵⁹ This is a highly controversial provision, and it is perhaps for this reason that, as noted

⁵² The Human Tissue Authority Code of Practice on Consent is a non-binding document that provides practical guidance to professionals carrying out activities within the scope of the Human Tissue Act. [hereinafter the Code]

⁵³ *Ibid.*, paragraph 40.

⁵⁴ *Ibid.*, paragraph 30. It is important to note, however, that from spring 2020 the current “opt-in” system of consent will be replaced by a new “opt-out” system.

⁵⁵ Broad consents, for example for “research purposes”, are deemed specific enough to be permissible. The Code, paragraphs 29, 48 and 51

⁵⁶ Section 5(1) HTA 2004.

⁵⁷ If a living adult lacks capacity to consent, consent can be deemed in some situations under the Human Tissue Act 2004 (Persons who Lack Capacity to Consent and Transplants) Regulations 2006.

⁵⁸ As per section 27(4) HTA 2004, possible qualifying relations are ranked in the following order: (a) spouse or partner; (b) parent or child; (c) brother or sister; (d) grandparent or grandchild; (e) child of brother or sister; (f) stepfather or stepmother; (g) half-brother or half-sister; (f) friend of long standing.

⁵⁹ See: Section 7(4) HTA 2004.

elsewhere, the UK Government has stated that it should only be utilised in extraordinary cases.⁶⁰ Research activities ethically approved in line with regulations issued by the Secretary of State for Health,⁶¹ material removed in the course of treatment,⁶² material imported from other jurisdictions,⁶³ and material obtained prior to the enactment of the HTA,⁶⁴ are all also exempt from the rules relating to individual consent.

In addition to specifying that removing, storing or using bodily material without consent is a criminal offence, the HTA also outlines a range of other associated offences. Falsey representing consent (e.g. claiming consent has been given when it has not),⁶⁵ using or storing donated material for an improper purpose,⁶⁶ and buying or selling bodily material,⁶⁷ are all behaviours that will result in prosecution.

4.2. The US Uniform Anatomical Gift Act 2006

The primary piece of legislation governing organ donation in the USA is the Uniform Anatomical Gift Act 2006.⁶⁸ The UAGA is a model act drafted by the Uniform Law Commission that must be passed into law by individual states to become active.⁶⁹ In apparent recognition of the need for a uniform approach to organ donation regulation, the UAGA has been enacted in every US state. Like the UK HTA, the UAGA establishes an opt-in system for organ donation. However, the legal principle central to the UAGA is gift law, as opposed to “consent” which, as noted above, plays a central role in the HTA.⁷⁰ Under the UAGA an (adult) individual can make an “anatomical gift” prior to their death,⁷¹ or such a gift can be authorised by an agent,⁷² a parent,⁷³ or a guardian⁷⁴ at the time of the individual’s death. Section 2(3) of the Act defines an “anatomical gift” as:

“...donation of all or part of a human body to take effect after the donor’s death for the purpose of transplantation, therapy, research, or education.”

A person can make a gift be made by authorising a statement indicating their desire to do so, by making a will expressing a desire to make a gift, or by expressing an intention to do so in any form of communication to at least two adult people, one of whom is a “disinterested witness.”⁷⁵ Anatomical

⁶⁰ Price, D. (2005) “The Human Tissue Act 2004”, *Modern Law Review*.

⁶¹ Sections 1(7)-(9) HTA 2004. These provisions bear some similarity to the Regulations considered above concerning access to medical data for research purposes.

⁶² Section 42 HTA 2004.

⁶³ Special provisions specify, however, that bodily material that is exported and then imported will fall outside the scope of this exemption.

⁶⁴ Section 9(4) HTA 2004.

⁶⁵ Section 5(2) HTA 2004.

⁶⁶ Section 8(4) HTA 2004.

⁶⁷ Section 32 HTA 2004.

⁶⁸ [hereinafter UAGA]

⁶⁹ The Uniform Law Commission is a body of law and policy experts appointed by the governors of each state to identify areas that would benefit from uniformity nationwide, but which cannot be federally regulated because they fall under the reserved powers of the state. Organ donation is one such area.

⁷⁰ On the significance of this nuance, see: Glazier, A. (2018) “Organ Donation and the Principles of Gift Law”, *Clinical Journal of American Society of Nephrology* 13(8), pp.1283-1284.

⁷¹ Section 4(1) UAGA

⁷² Section 4(2) UAGA

⁷³ Section 4(3) UAGA

⁷⁴ Section 4(4) UAGA

⁷⁵ Section 5 UAGA. “Disinterested witness” is defined by section 2(5) of the Act as a person other than the spouse, child, parent, sibling, grandchild, grandparent, or guardian of the donor.

gifts can be revoked via a record signed either by the donor themselves or their surrogate, or another person acting on their behalf.⁷⁶

Section 9 of the Act specifies that any member of the classes of persons listed below may authorise an anatomical gift from the body of a deceased person, for the purpose of transplantation, therapy, research or education. These are listed by the Act in order of priority (i.e. the wishes of a person in a lower-ranked class cannot triumph over those of a person in a higher class):

- An agent of the deceased;
- The spouse of the deceased;
- Adult children of the deceased;
- Parents of the deceased;
- Adult siblings of the deceased;
- Adult grandchildren of the deceased;
- Grandparents of the deceased;
- An adult person who has exhibited special care for the deceased;
- A person acting as guardian for the deceased at the time of death;
- Any other person having the authority to dispose of the deceased's body (e.g. a coroner or medical professional).

Another point of interest is the way in which the UAGA places a range of positive statutory duties on certain third parties, in addition to the rules relating to donors themselves and people making decisions on their behalf. Police officers, firefighters, and paramedics, for instance, must, when encountering a deceased person, or a person who is close to death, make a reasonable search for a document outlining the person's intentions regarding whether to make a gift.⁷⁷ If this is located, and the person in question is sent to hospital, the document must also be sent. Breach of this duty is not a criminal offence but may be subject to administrative sanctions and civil penalties. Hospitals, and their staff are placed under a similar duty to refer individuals who are close to death to an organ procurement organisation, which will then search for the records of the individual to determine whether they are a registered donor.⁷⁸

Like the HTA, the UAGA also outlines some specific criminal offences that may be committed in the context of bodily material and the handling thereof. Specifically, any person who knowingly sells or purchases a human body, or any part of a body, will incur criminal liability for doing so.⁷⁹ Falsifying, forging, concealing, defacing or obliterating a document authorising or revoking a gift will also be a crime.⁸⁰

5. Lessons to be learned?

The previous section revealed numerous consistent themes between UK and US organ donation regimes. The purpose of this section is to consider the significance of some of these themes and evaluate their possible salience in the context of designing a regulatory framework for PMDD.

⁷⁶ Section 6 UAGA.

⁷⁷ Section 12 UAGA.

⁷⁸ Section 14 UAGA

⁷⁹ Section 16 UAGA

⁸⁰ Section 17 UAGA

5.1. The role of the individual

Perhaps the most significant question to be asked regarding the construction of a bespoke regulatory framework for PMDD relates to the role of the individual and the extent to which their consent, authorisation, or preferences more generally, should play a role. As outlined above, the default position under both the HTA and UAGA is that the removal of bodily material without the consent or authorisation of the relevant individual, or appropriate proxy, will be unlawful. To this end, the individual is afforded a position of considerable influence. Should this also be the default position regarding posthumous donations of medical data? Should the consent or authorisation (either opt-in or opt-out) of the individual ordinarily be required for medical data to be donated and stored posthumously? The obvious answer to these questions is perhaps yes. Basing a PMDD regulatory framework around the ideals of individual autonomy and control, for example, would ensure its alignment with the growing EU policy rhetoric associated with affording individuals greater control over their personal data.⁸¹

However, this would not be without controversy. As noted elsewhere, the way in which organ donation laws place such great emphasis on the wishes of individuals, even post-death, is a persistent source of criticism. Various observers have argued, for instance, that such an approach unjustly prioritises the wishes of the deceased person over the needs of the living.⁸² Bodily material, for example, may be extremely valuable in the context of communal or societal purposes, most obviously in the context of organ donation. To such observers, for the law to allow such purposes to be defeated by the wishes of a person who is no longer alive, and thus has no need for their bodily material, is completely unacceptable. Their view, therefore, is very much that the law should not require consent or authorisation in order for the bodily material of deceased persons to be extracted and used.⁸³

The main counter arguments to this position are built around the idea that if the law allows individuals to make testamentary dispositions in respect of their real and personal property, they should also be allowed to make dispositions regarding their bodies. The ability to make testamentary dispositions regarding real or personal property is often justified by way of reference to a personal connection an individual has with their material possessions. Bodily material, on the other hand, is by its very nature more intrinsically linked to an individual's personhood than material possessions. Ergo, it would be illogical for the law, because of the existence of a personal nexus, to allow posthumous control over the former but not the latter.⁸⁴ In a similar vein, others have argued that ignoring a person's wishes regarding what happens to their body post-death can cause them harm whilst they are still alive, thereby necessitating a regulatory approach conducive to individual control and autonomy.⁸⁵

It is not difficult to see how such debates could come to be replicated in the context of the construction of a PMDD regulatory framework. Personal data, like bodily material, as outlined above, are intrinsically linked to an individual's personhood, but the processing of such data for research purposes may also be of huge value to the community. If an individual were to refuse for their data to be donated to a particular recipient, or for a particular purpose, questions in the “*why should the*

⁸¹ On this issue, see: Lazaro, C. and Le Metayer, D. (2015) “The control over personal data: True remedy or fairy tale?”, *SCRIPTed* 12(1), pg.6.

⁸² See, particularly: Harris, J. (2002) “Law and regulation of retained organs: the ethical issues”, *Legal Studies*; Harris, J. (2003) “Organ procurement: dead interests, living needs”, *BMJ*. Bird, S. and Harris, J. (2010) “Time to move to presumed consent for organ donation”, *BMJ*.

⁸³ *Ibid*

⁸⁴ See, particularly: Brazier, M. (2002) “Retained organs: ethics and humanity”, *Legal Studies*; Brazier, M. (2015) “The body in time”, *Law, Innovation and Technology*.

⁸⁵ *Ibid*

wishes of the dead be capable of trumping the interests of those still living?" vein could quite conceivably arise. Despite such debates, it is surely likely that individual autonomy would play a focal role in a PMDD regulatory framework. Any divergent approach would immediately be at odds with the general thrust of data protection law, which, as alluded to above, has become increasingly geared towards establishing individual control of personal data. Whilst the consent or authorisation of the individual would surely play a focal role, however, a balance between individual and communitarian interests would clearly need to be struck. Precisely where, and how, that balance would be struck, however, would likely be contested. It is not immediately obvious, for instance, that the same reasons frequently invoked as a justification for affording individuals control and autonomy over their personal data in life would be equally applicable to situations relating to posthumous control, perhaps particularly given the abovementioned societal benefits the processing of such data may have.⁸⁶

5.2. Scope

A second salient question that stems from the first (considered above) is that assuming the consent or authorisation of a relevant individual would generally be required for data to be donated under a PMDD regulatory framework, what should the scope of that framework be? Should, for instance, consent or authorisation be required for the donation or acquisition of *all* of an individual's medical data? Or, should such requirements only be imposed on data of particular character or sensitivity? To place these questions in context, it is worth noting that in relation to the HTA, various observers have criticised the scope of its definition of "bodily material". It has been suggested, for instance, that the breadth of such terms can impede or prevent the donation of material that would be significant for communal purposes (e.g. medical research), but would be of no significance to the individual from which they would be extracted.⁸⁷ For instance, the HTA's definition of bodily material is broad enough to encompass a tiny amount of skin cells, which arguably would be of concern to nobody. This raises questions regarding whether it makes sense for consent to be required for the extraction of such material.

Similar observations can be made in respect of precisely which medical data should fall within the scope of a PMDD regulatory framework. Whilst some medical data might be of significant concern to individuals and would warrant inclusion, it is not immediately obvious that the same could be said of *all* medical data. Research has established, for instance, that individuals place much greater importance on the security and integrity of certain types of personal data than others.⁸⁸ For example,

⁸⁶ For the counter argument to this position, see: Harbinja (n 23)

⁸⁷ See, for instance: Skene, L. (2002) "Ownership of human tissue and the law", *Nat Rev Genet*; Laurie, G. and Mason, K. (2001) "Consent or Property: Dealing with the Body and its Parts in the Shadow of Bristol and Alder Hey", *Modern Law Review*.

⁸⁸ See, for example: The Wellcome Trust (2013) "Summary Report of Qualitative Research Into Public Attitudes to Personal Data and Linking Personal Data", available at: https://mesh.tghn.org/site_media/media/articles/Qualitative_Research_into_Public_Attitudes_to_Personal_Data_and_Linking_Persona_FLr04DM.pdf; Ipsos MORI (2014) "Privacy and personal data", available at: <https://www.ipsos.com/sites/default/files/migrations/en-uk/files/Assets/Docs/Polls/jrrt-privacy-topline-nhs-2014.pdf>; ICO (2014) "Annual Track 2014", available at: <https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf>; Eurobarometer (2015) "Data Protection", available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf; ICO (2015) "Data protection rights: What the public want and what the public want from Data Protection Authorities", available at: <https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf>; DMA (2015) "Data privacy: what the consumer really thinks", available at: https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf; ODI (2018) "ODI/YouGov Poll Results – Attitudes towards data sharing", available at: <https://theodi.org/blog/odi-survey-reveals-british-consumer-attitudes-to-sharing->

raw personal data relating to an individual's health status are widely thought to be of greater concern than metadata relating to email communications, including those with a doctor or hospital, yet both data types are "personal" for the purposes of data protection law.⁸⁹ Whether there would be a need or justification for requiring authorisation or consent to be obtained prior to the donation or acquisition of all types of medical data is, therefore, an important question. Precisely how such a framework would approach situations involving data that had nominally been anonymised, and situations in which the storage of medical records is fragmented, are other closely related issues that would also need to be considered in detail.⁹⁰

5.3. Exceptions

Though the central notion of both organ donation regulatory frameworks considered above is that either consent or authorisation must be obtained before the extraction of bodily material is permitted, this is clearly not an absolute principle. The HTA in particular outlines a number of exceptional circumstances where bodily material can be extracted posthumously without consent. Notably, for example, as outlined above, in the absence of consent being given the HTA allows for consent to be inferred by the Human Tissue Authority, and for the High Court to order extraction. Assuming a regulatory framework for PMDD was built around the notion of individual autonomy, as outlined above, should it too contain a list of exceptions to this central principle, and, if so, what should the exceptions be?

Logically, the answer is yes. As alluded to above, though data protection law aims to affirm an individual's sovereignty over their personal data, this sovereignty is far from absolute. The fact that the consent of the individual is only one of the grounds listed in the GDPR through which the processing of personal data can be legitimised clearly shows this.⁹¹ Similarly, the GDPR also provides that certain data processing activities in which there is a communal interest will not have to comply with the data protection principles and other substantive data protection rules. Data processing undertaken for national security purposes, for instance, is explicitly stated to fall outside the scope of the GDPR.⁹² So to correlate with the main tenets and general thrust of the data protection law it would make sense for a PMDD regulatory framework to operate on a similar basis, providing for some situations in which the consent or authorisation of the individual would not be required for donation, and some activities that fall outside its scope. For example, consent or authorisation not being required for posthumous data handling in the context of criminal investigations, or possibly in the context of journalistic activities.

Whilst this approach would be *prima facie* sensible, however, the experience of the organ donation regulatory regimes considered above suggest it would not necessarily be free from controversy. For example, as noted above, the main goal of the HTA and other comparable legislation is to enhance

personal-data-online. See also: Addae, J. (2017) et al. "Measuring attitude towards personal data for adaptive cybersecurity", *Information & Computer Security*, available at:

<http://www.emeraldinsight.com/doi/pdfplus/10.1108/ICS-11-2016-0085>

⁸⁹ *Ibid*

⁹⁰ On the data-protection related difficulties that may arise in conjunction with efforts to anonymise personal data, see: Rocher, L. Hendrickx, J. and de Montjoye, Y. (2019) "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*. See also: Pearce, H. and Stalla-Bourdillon, S. (2019) "Rethinking the "release and forget" ethos of the Freedom of Information Act 2000: Why developments in the field of anonymisation necessitate the development of a new approach to disclosing data", *European Journal of Law and Technology* 10(1).

⁹¹ Article 6 GDPR.

⁹² Recital 16 GDPR.

individual autonomy and posthumous-control of bodily material. The construction of a bespoke regulatory regime for PMDD would likely aspire to do the same in respect of individuals' personal data. However, as remarked in the literature, the existence of a long list of exceptions contained within the HTA arguably undermines this objective.⁹³ Legal rules that aim to affirm autonomy will inevitably have limited value, for instance, if they are subject to a range of exceptions so extensive it makes it impossible for them to gain traction. Others have suggested that it is not clear what the Act is trying to achieve, and that it is a piece of legislation in conflict with itself. By attempting to give effect to both individual (i.e. through consent) and communal interests (i.e. through the listed exceptions), so the argument goes, the Act, in fact, does neither, and thus is a confused and incoherent piece of law.⁹⁴ As noted in the literature, a lack of clarity can be extremely damaging to the efficiency and legitimacy of any regulatory regime.⁹⁵ Accordingly, this is a pitfall it will be important for any PMDD regulatory framework to avoid.

5.4. Criminal liability

Both the HTA and the UAGA outline numerous criminal offences that can be committed via the inappropriate handling of bodily material, misrepresentation of consent/authorisation, and various other behaviours. Though the HTA is more extensive than the UAGA and articulates a wider range of offences, both regimes clearly envisage criminal penalties as an appropriate means of redress for non-compliance. The question that naturally stems from this, therefore, is whether a regulatory framework for PMDD should also operate on such a basis. In other words, should non-compliance with such a framework, for instance via the inappropriate handling of the data of a deceased person, result in criminal liability? If the mishandling of bodily material is deserving of criminal sanction due to the way in which they are intrinsically linked to an individual's personhood and identity then arguably the answer is yes. After all, personal data can be described in the same way, and thus their mishandling post-death should arguably be treated similarly.

Perhaps in correlation with this manner of thought, the UK's recently enacted Data Protection Act 2018 contains some novel and bespoke criminal offences relating to inappropriate treatment of individuals' personal data. Section 171 of the Act, for instance, introduces a new offence that will be committed when a defendant knowingly or recklessly de-anonymises anonymised data without the consent of the data controller responsible for the anonymisation.⁹⁶ If the trend of using criminal law as a means of resolving data protection issues is to continue, then perhaps it would make sense for a PMDD regulatory framework to be underpinned by criminal penalties. However, this would require careful thought. Though the use of criminal law in this context might be *prima facie* appealing it is a possibility that is inherently problematic. As noted elsewhere, the use of criminal law requires clear and precise legal norms that are often not available in data protection. Data protection crimes also face competition from "normal" crimes (e.g. theft, assault, criminal damage etc.) for enforcement resources, and their prioritisation is perhaps doubtful. A lack of technological expertise on the part of

⁹³ Herring, J. and Wall, J. (2017) "The Nature and Significance of Bodily Integrity", *Cambridge Law Journal*.

⁹⁴ Parker, L. (2011) "Using human tissue: when do we need consent?" *Journal of Medical Ethics*; , Harmon, S. and McMahon, A. (2014) "Banking (on) the brain: From consent to authorisation and the transformative potential of solidarity", *Medical Law Review*.

⁹⁵ Brownsword, R. and Goodwin, M. (2012) *Law and the Technologies of the Twenty-First Century*, Cambridge: Cambridge University Press. See also: Murray. A. (2019) *Information Technology Law*. Oxford: Oxford University Press.

⁹⁶ See note 92 for some useful considerations of anonymisation and its pitfalls.

law enforcement bodies and the judiciary would also likely lead to a muddled approach and unsatisfactory results.⁹⁷

6. Conclusion: beyond ethics - the law of posthumous data donation?

In this section, we make some tentative suggestions for legislative/policy reforms that would enable the practice of PMDD. Our recommendations would make the law regarding access to health records by researchers more coherent. Before venturing into that discussion, we summarise the main findings of this paper, so to clarify the bases for our suggestions.

In principle, the legal treatment of personal data of living and the deceased individuals, including patients' records, is not based on property and ownership, but rather, protection is offered through general data protection regimes, sector-specific data protection regimes, and the doctor/patient duty of confidence. General data protection regimes do not apply to deceased individuals in either of the analysed countries. In terms of sector-specific laws, the US system appears clearer and more conducive to PMDD, with some discrepancies at the state level. The HIPAA offers options for researchers to access PHI of the deceased, unlike English law where the permissibility of such access is unclear from sector-specific legislation. General data protection rules do not apply to the deceased, so the research exemption outlined in the GDPR similarly does not apply. The NHS Act offers more clarity, but the use of deceased's medical data can be trumped by her consent for use for other specific purposes. This, unfortunately, has not been developed further in the policy. Doctor to patient confidentiality seems to extend beyond death in England, so this, in principle, is capable of preventing disclosure of medical data and patient records. The 2002 Regulations allow for the duty of confidence to be set aside in certain situations, but this can be further trumped by the deceased's consent or her opt-out. Therefore, it seems necessary to amend the existing legislation and policies in order to provide for a clear PMDD framework. An analysis of the regulatory position regarding organ donation helps to cast light on how best to develop such a framework but also reveals a number of pitfalls and challenges that such a framework would have to avoid and negotiate. In particular, questions relating to the role of the individual (and the need for their consent), the scope of such a framework, its exceptions, and the utilisation of criminal law, could all prove to be problematic.

In order to make the possibility of PMDD clear and coherent in English law, the following key amendments would be required. In particular, The Access to Health Records Act 1990 and the Public Records Act 1958 would need to at least mention PMDD, so to enable access for research purposes with the deceased's consent. At present, under general data protection law, consent is not required, since the deceased is not data subjects according to the DPA 2018. This position would require adjustment. Consent should be also introduced through ethical codes, such as the Code for Posthumous Medical Data Donation mentioned in section 1.⁹⁸ One possibility is to align such consents with a standard commensurate with that used by data protection and organ donation legislation, so that the deceased's consent, expressed pre-mortem, must be freely given, informed and unambiguous, by a statement or by a clear affirmative action, whereby an individual signifies agreement with PMDD. This is in line with article 4(11) of GDPR, though it omits the word 'specific' if the deceased chooses to donate their data for any research purpose, as long as it is for non-

⁹⁷ On this issue, see: Brownsword, R. and Goodwin, M. (2012) *Law and the Technologies of the Twenty-First Century*, Cambridge: Cambridge University Press.

⁹⁸ Krutzinna J., Taddeo M., Floridi L. (2019) "An Ethical Code for Posthumous Medical Data Donation" in: Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer, Cham

commercial research. The Access to Health Records Act 1990 should be amended to allow for access by researchers when permitted by the deceased or their personal representative. Amendments to the NHS Act along these lines would also be helpful, and the option for PMDD should be clearly set out. This would not affect the common law duty of confidence, as the option would include the deceased's consent. In America, HIPAA could be amended to include PMDD as well. In order to clarify ethical processes, HIPAA could also state explicatively that further consent from the next of kin or personal representative is not required in the case of PMDD.

Another idea would be to look at PMDD more holistically and for the Secretary of State for Health to introduce separate regulations for the UK, which would amend the relevant laws and set out the general principles of PMDD, including the recognition of ethical codes and the NHS policies. If this option was pursued, the questions considered above in section 5 would be highly pertinent. Careful thought would, for instance, need to be given to questions relating to whether donation would only be permitted in respect of certain purposes (e.g. for commercial, rather than non-commercial, purposes), whether and in what situations a relative or proxy could give consent on behalf of the deceased and in what circumstances, and whether it would be possible to consent to the donation of some data whilst excluding other types. In a similar vein, questions regarding the utilisation of criminal law, and whether, and in what circumstances, criminal penalties should be levied against those mishandling health data post-mortem also may require address.

One final question that is of a technical, rather than legal, nature, relates to how a PMDD regulatory framework could be operated from a technological perspective. In other words, what technologies could be used, or would be needed, to underpin and support a regulatory framework for PMDD? To this end, it has been suggested that democratically controlled non-profit personal data cooperatives may help to establish a governance and trust framework for data sharing and data donation.⁹⁹ In a similar vein specific technological tools, such as personal data stores, as mechanisms which allow individuals to control their personal data transactions, may also have the potential to contribute to the achievement of this objective.¹⁰⁰ Whatever technology, or technologies, are ultimately used to help facilitate PMDD, however, challenges pertaining to standardisation and interoperability, digital

⁹⁹ Hafner E. (2019) "Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health" in: Krutzinna J., Floridi L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer, Cham

¹⁰⁰ On the use of personal data stores, see: Van Kleek, Max and O'Hara, Kieron (2014) *The future of social is personal: the potential of the personal data store*. In, *Daniele Miorandi, Vincenzo Maltese, Michael Rovatsos, Anton Nijholt & James Stewart (eds.), Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society*. Heidelberg, DE. Springer Verlag, pp. 125-158. See also: Pearce, H. (2015) "Online Data Transactions, Consent and Big Data: Technological Solutions to Technological Problems?", *Computer and Telecommunications Law Review* 22(4).

literacy, scalability, fair competition and cybersecurity will all likely need to be wrestled with.¹⁰¹ There may also be other underlying ethical concerns associated with the use of technology in this context.¹⁰²

¹⁰¹ On these issues, see: De Filippi, P. (2016) "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production*. Available at: <http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain->; Wright, A. and De Filippi, P. (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664; Goldsmith, J. and Wu, T. (2006) *Who Controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press; Wu, T. (2012) *The Master Switch: The Rise and Fall of Information Empires*, London: Atlantic Books; Crosby, M. et al. (2015) "Blockchain Technology: Beyond Bitcoin", *Sutardja Center for Entrepreneurship & Technology Technical Report*, pg.3; Bondi, A. (2000) "Characteristics of scalability and their impact on performance", *Proceedings of the second International Worksop on Software and Performance*, pg.195; Heath, W. (2014) "Personal Data Stores", *Society for Computers and Law.*; Jenkins, H. (2009) *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*, Cambridge, Massachusetts: MIT Press; Sunstein, C. (2014) "Active Choosing or Default Rules? The Policymaker's Dilemma", available at: https://dash.harvard.edu/bitstream/handle/1/12186290/activechoosingpaternalism5_14.pdf?sequence=1; Jensen, M. (2013) "Challenges of Privacy Protection in Big Data Analytics", *2013 IEEE Congress on Big Data*; Narayanan, A. et al. (2012) "A Critical Look at Decentralized Personal Data Architectures", available at: <http://arxiv.org/pdf/1202.4503v1.pdf>.

¹⁰² On this issue, see: Brownsword, R. "So What Does the World Need Now? Reflections on Regulating Technologies" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, ed. by Brownsword, R. and Yeung, K. (2008) Oxford: Hart. pg.38; Brownsword, R. (2008) *Rights, Regulation and the Technological Revolution*, Oxford: Oxford University Press.