

Volume 10, Issue 1, April 2013

DOES THE EU DATA PROTECTION REGIME PROTECT POST-MORTEM PRIVACY AND WHAT COULD BE THE POTENTIAL ALTERNATIVES?

Edina Harbinja^{*}

Abstract

This article aims to shed some light on post-mortem privacy, a phenomenon rather neglected in the legal literature. Acknowledging the quite controversial nature of the phenomenon and certain policy and legal arguments pro and contra, the paper explores the data protection (informational privacy) aspect of the issue. More precisely, the focus is on the distinction between the current and the newly proposed data protection regime in the European Union (EU), assessing how these regimes are susceptible to protecting the deceased's personal data. The paper will note the differences between the proposed text of the Data Protection Regulation Proposal and subsequent amendments. Moreover, the paper will assess which solutions are more suitable to enable incorporation of the post-mortem privacy in the data protection regime, acknowledging the overall lack of certainty regarding the finalisation of the Regulation's content. In so doing, this paper aims to detect elements in the new regime that seem to be promoting, at least theoretically, the propertisation of personal data, while partly disregarding its human rights basis. Having this assumption in mind and noting the difference between property, liability and contracts regimes (e.g. transmission on death), it will be argued that the new regime, at least in theory, could be perceived as promoting post-mortem privacy and, under certain circumstances,

^{*} PhD Candidate, University of Strathclyde, Law School, contact: e.harbinja@strath.ac.uk. The research is funded by the Horizon Digital Economy Hub, Nottingham, for which the author expresses her gratitude; and forms part of the work programme of the RCUK funded Centre for Creativity, Regulation, Enterprise and Technology (CREATE – see www.create.ac.uk). A version of this paper was delivered at the Amsterdam Privacy Conference 2012 panel on *Death and Post-Mortem Privacy in the Digital which Age*, which the author co-organised. The author would like to acknowledge the helpful comments and feedback received at the conference. Special gratitude goes to Prof. Lilian Edwards, University of Strathclyde, for her assistance, support and valuable comments relating to this article. The author also thanks an anonymous commenter for additional feedback. Any errors that remain are the sole responsibility of the author.

enabling better control of deceased people's personal data. The paper, however, does not support this change and suggests that post-mortem privacy should be contemplated within the human rights-based regime.

DOI: 10.2966/scrip.100113.19



© Edina Harbinja 2013. This work is licensed under a [Creative Commons Licence](#). Please click on the link to read the terms and conditions.

1. Introduction

Post-mortem privacy (deceased persons' privacy), has been, so far, a phenomenon of interest predominantly for sociologists, psychologists, anthropologists and other humanities and social sciences scholars.¹ It has not been, however, such an interesting subject of research for legal academics and does not represent a term of art in the legal profession (not even amongst privacy scholars).² This issue, nevertheless, deserves the attention of legal scholarship, bearing in mind the development of technology, the accompanying social relations, and all the possible interests and values at stake. Some of those rather conflicting interests will be touched upon in the following section.

The growth of the Internet-enabled ubiquitous technologies has led to the growth of "digital natives,"³ along with the storing of enormous amount of digital assets and personal data online. The number of digital natives worldwide is significant,⁴ and the effect and importance of their digital identities cannot be disregarded. A significant number of them die every day.⁵ Some of them would like to see their wishes as to

¹ See e.g. C J Sofka, K R Gilbert and I N Cupit (eds), *Dying, death and grief in an online universe* (New York: Springer Publishing Company, 2012); B Carroll and K Landry "Logging on and letting out: Using online social networkings to grieve and to mourn" (2010) 30(5) *Bulletin of Science, Technology & Society* 341-349; D Klass "Continuing conversations about continuing bonds" (2006) 30 *Death Studies* 843-858.

² With exceptions such as for example: Amsterdam Privacy Conference 2012, *Panel on Death and Post-Mortem Privacy in the Digital Age*, 8 Oct 2012, *Chair*: Lilian Edwards, *Panellists*: Edina Harbinja, Anna E. Haverinen, Damien McCallig, Elaine Kasket, available at http://www.apc2012.org/sites/default/files/pdffiles/APC%20programme_0.pdf (accessed 10 Jan 2013) or L Essers "Online Life After Death Faces Legal Uncertainty" CIO, 08 Oct 2012 available at http://www.cio.com/article/718253/Online_Life_After_Death_Faces_Legal_Uncertainty (press report on the panel) (accessed 10 Jan 2013). The panel was not purely legal in character, but rather interdisciplinary with legal observations amongst others. For the US perspective see e.g. M Wilkens "Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?" (2011) 62 *Hastings Law Journal* 1037-1064; J Atwater "Who Owns E-mail? Do You Have the Right to Decide the Disposition of Your Private Digital Life?" (2006) 2 *Utah Law Review* 397-418; J J Darrow and G R Ferrera "Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?" (2007) 10 *New York University Journal of Legislation and Public Policy* 281-320.

³ Palfrey and Gasser, for instance, define digital natives as a population that satisfy the following criteria: born after the year of 1980; have access to digital technology; and have skills to use digital technology "in relatively advanced ways". J Palfrey and U Gasser "Reclaiming an Awkward Term: What we Might Learn from "Digital Natives"" (2011) 7 *A Journal of Law and Policy for the Information Society* 33-56, at 37-38; Cheatham defines digital natives as a generation that has never known a world without digital technologies. C Cheatham "Public Relations: Dancing with Digital Natives: A Great Resource for Understanding Those Who Have Grown up with Digital Technology" (2011-2012) 16 *AALL Spectrum* 8-10.

⁴ For example, the number of Facebook users has reached more than a billion worldwide, see Facebook, Key facts, "One billion monthly active users as of October 2012" available at <http://newsroom.fb.com/Key-Facts> (accessed 10 Jan 2013).

⁵ For instance, research suggests that approximately 375,000 Facebook users in the United States die every year. J Mazzone "Facebook's Afterlife" (2012) 90 *North Carolina Law Review* 1643-185, at

what happens to their personal data after death respected.⁶ These wishes could, however, clash with the wishes and interests of society, of theory, and of families and friends, as seen in the scarce case law (discussed in the following section).

The phenomenon of post-mortem privacy can be contemplated from the perspective of privacy in general, or of informational privacy more specifically (i.e. protection of personal data).⁷ It has, however, many other implications and angles, such as protection of personality rights, author's moral rights, dignity, defamation, libel, organ donation and other strictly personal rights and claims. The focus of this paper will be on the informational aspect of privacy (data protection) and its legal implications within the current (the *Data Protection Directive*⁸ and some national rules) and perspective data protection regime(s).

The issue of what happens to the deceased's data and individuals' privacy post-mortem is far from clear and settled from a legal and regulatory perspective. Currently, most of the data protection regimes do not include protection of decedents' personal data and they do not legally recognise this aspect of "post-mortem privacy". Therefore, the question arises as to whether personal data should be protected both in life and upon death.

Notwithstanding the conflicts that might arise, this paper seeks to explore if it would be legally viable to recognise the deceased's right to privacy at the EU level. Deceased person's privacy is discussed herein in the context of their personal data, and whether this data should be protected through data protection legislation, acknowledging that the concept of "the deceased's right to privacy" is broader and includes, *inter alia*, data protection. The broader conception of "post-mortem privacy"

1647; more specifically see N Lustig "2.89m Facebook Users Will Die in 2012, 580,000 in the USA" 6 June 2012, Natan Lustig Blog, at <http://www.nathanlustig.com/2012/06/06/2-89m-facebook-users-will-die-in-2012-580000-in-the-usa/> (accessed 20 Feb 2013)

⁶ Apart from the interest amongst humanities and social sciences scholars, the issue had been of a wide media interest in the past few years, thus raising awareness amongst the Internet users and making them ask questions about its legal implications. See J Hopper, "Digital Afterlife: What happens to your online accounts when you die?" Rock Center, 01 Jun 2012, available at <http://rockcenter.nbcnews.com/news/2012/06/01/11995859-digital-afterlife-what-happens-to-your-online-accounts-when-you-die?lite> (accessed 05 Jan 2013); E Carroll, "What happens to your Facebook account when you die?" The Digital Beyond 07 Feb 2012 available at <http://www.thedigitalbeyond.com/2012/02/what-happens-to-your-facebook-account-when-you-die/> (accessed 05 Jan 2013); J Shah, "Digital Life After Death: America One Step Ahead. On your passing, your online presence will remain. But should it?" *Morrison's solicitors* 22 Feb 2012 available at <http://www.morrilaw.com/news/digital-life-after-death-america-one-step-ahead> (accessed 05 Jan 2013); R. Herold, "How to Protect Your Privacy After You Die" Infosec island 06 Apr 2010 available at <http://www.infosecisland.com/blogview/3537-How-to-Protect-Your-Privacy-After-You-Die.html> (accessed 05 Jan 2013) etc.

⁷ Privacy can be further conceived as the right to be let alone; privacy as a limited access to the self; privacy as secrecy; privacy as personhood or privacy as intimacy. See e.g. D J Solove, "Conceptualizing privacy" (2002) *California Law Review* 1087-155, at 1093.

⁸ *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995 p. 0031 – 0050.

and its legal protection is sketched briefly in the following section. After this general discussion, the paper assesses the current and newly proposed data protection regime in the EU in relation to the deceased's data. It aims to explore whether the deceased's privacy could be protected within the current data protection framework or the proposed regulation⁹ would be a more suitable instrument to achieve this goal. It further identifies some elements of the *propertisation* of personal data in the proposed regime. In the next sections, the paper questions whether the regime would depart, to some extent, from its human rights basis to *commodification* and *propertisation* of personal data. If this proves correct, then the new regime could be deemed favourable to post-mortem privacy, since property entails transfer in life and on death, whereas torts or liability regimes mainly protect the living.

However, it is argued here that this move would not be the best solution, neither for the protection of personal data of the living, nor for the protection of the deceased's data. The regime should aim to operate from a human rights basis; solutions for protecting post-mortem privacy should be sought within that framework. The paper therefore suggests that the real improvement would be an explicit introduction of post-mortem privacy protection in the proposed Regulation. Noting the direct effect of a regulation in all the EU member states, this change would harmonise regimes, and enable the same level of protection for EU users and their personal data.

The precisely defined solutions are, however, beyond the scope of this paper. It does not aim to provide all the answers to why stronger post-mortem privacy protection is desirable, as this will be subject to a broader discussion and a careful policy choice, weighing cautiously post-mortem privacy with other rights, values and interests, as suggested briefly in the next section. This paper could perhaps serve as a starting point for these broader considerations.

2. Some controversies surrounding post-mortem privacy

Post-mortem privacy, at a legal conceptual level, could refer to various different areas of law (e.g. human rights, property, succession, personality rights, intellectual property, etc.). In all these areas there is a different legal attitude towards the dead, in addition to the differences between legal systems. Some of the major ones will be presented briefly.

In the English common law system, for instance, there is a long recognised principle of *actio personalis moritur cum persona* (personal causes of actions die with the person, e.g. defamation claims, breach of confidence claims),¹⁰ implying the negative attitude towards rights of the dead. However, this attitude in common law does not

⁹ *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, 2012/0011 (COD), 25.1.2012.

¹⁰ Established in *Baker v Bolton* (1808) 1 Camp. 439; 170 ER 1033. The principle has been revised in the UK and now only pertains to causes of action for defamation and certain claims for bereavement. See the *Law Reform (Miscellaneous Provisions) 1934 Act c. 41*, *Race Relations Act 1976 c. 74*, *Sex Discrimination Act 1975 c. 65*, *Disability Discrimination Act 1995 c. 50* and *Administration of Justice Act 1982 c. 53*.

pertain to, for instance, moral rights of authors. In the United Kingdom (UK), moral rights subsist as long as copyright in work subsists (including the right to privacy of certain photographs and films), except for the right against false attribution of work, which lasts until 20 years after a person's death.¹¹

On the other hand, many EU member states are of the civilian tradition which has historically been more inclined to recognise the persistence of similar rights after death. This protection regards privacy in a broader sense, dignity and moral rights of authors. For example in the German *Mephisto*¹² and *Marlene Dietrich* cases¹³, the courts granted protection for both the non-commercial (dignity, privacy) and commercial interests of the deceased (the use of name, voice, or image for financial gain).¹⁴ However, the French courts took a different position. In the case of *SA Editions Plon v Mitterand*,¹⁵ Court of Cassation held that “the right to act in respect of privacy disappears when the person in question, the sole holder of that right, dies”. The position of civilian systems towards moral rights of creators is, however, much clearer and it consists of stronger and more persistent rights. In France, for instance, creators' moral rights are perpetual, as a consequence of the dualistic conception of copyright (i.e., a separate treatment of economic and moral rights); in Germany, moral rights last as long as economic rights, as a consequence of a monistic conception.¹⁶

¹¹ See s 77 – 86 *Copyright, Designs and Patents Act 1988 c. 48* and commentary in L Bently and B Sherman *Intellectual property law*, 3rd ed (Oxford: Oxford University Press, 2008), at 167; or H L MacQueen et al. *Contemporary intellectual property: law and policy* (Oxford: Oxford University Press 2011), at 104 – 118.

¹² *Mephisto*, BVerfGE 30, 173, Federal Constitutional Court (First Division), 24 February 1971, translated by J. A. Weir: “It would be inconsistent with the constitutional mandate of the inviolability of human dignity, which underlies all basic rights, if a person could be belittled and denigrated after his death. Accordingly an individual's death does not put an end to the state's duty under Art. 1 I GG to protect him from assaults on his human dignity”, available at: The University of Texas at Austin, School of Law, Institute for Transnational Law, Foreign Law Translations, http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=1478 (accessed 03 Apr 2013).

¹³ *Marlene Dietrich Case* BGH 1 ZR 49/97, 01 December 1999, translated by Raymond Youngs, available at: The University of Texas at Austin, School of Law, Institute for Transnational Law, Foreign Law Translations, http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=726 (accessed 03 Apr 2013).

¹⁴ *Ibid.* Judgment states: “...b) The components of the right of personality which are of financial value remain after the death of the holder of the right of personality, at any rate as long as the non-material interests are still protected. The corresponding powers pass to the heir of the holder of the personality right and can be exercised by him in accordance with the express or presumed will of the deceased.”, at http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=726 (accessed 03 Apr 2013).

¹⁵ *SA Editions Plon v. Mitterand* (Civ. 1, 14 December, 1999, Bull. no. 345), Translated French Cases and Materials under the direction of Professor B. Markesinis and M. le Conseiller Dominique Hascher, Translated by: Tony Weir available at http://www.utexas.edu/law/academics/centers/transnational/work_new/french/case.php?id=1240 (accessed 10 Jan 2013).

¹⁶ For a useful comparison between English, French and German law attitudes to moral rights see S Newman, “The development of copyright and moral rights in the European legal systems” (2011) 33(11) *European Intellectual Property Review* 677-689.

Therefore, looking at these aspects of a general conception of privacy, there are perhaps more arguments for the protection of post mortem privacy than against this protection.

Conversely, the legal conception of privacy as a human right (Article 8 of the European Convention on Human Rights), does not really offer arguments for the proponents of post-mortem privacy protection. According to the European Court of Human Rights case law, Article 8 grants protection only to the living.¹⁷ In numerous cases, the Court has refused to recognise this right to the deceased, unless their privacy is connected to the privacy of the living individuals.¹⁸

The topic is therefore rather controversial and there is not a simple answer to the question of whether personal data of the deceased— a narrow conception of post-mortem privacy, should be protected. At a policy level, the proponents of legal recognition of this phenomenon could argue that there should be some form of protection for the deceased's privacy, since they are not able to shape their public image and protect their dignity. Also, some could argue, that pursuant to the principle of freedom of testation, that the wishes of the deceased should be respected and that protecting the privacy of the deceased also protects the mourning family. Conversely and understandably, these persons are subject to less harm, so the protection should not equate to the protection granted to living persons, if it is to be awarded at all.¹⁹ Moreover, the assumed interests of the deceased could conflict with the interests of their family and friends as acknowledged in United States (US) case law.²⁰ In these cases, the privacy interests of the deceased prevailed over the requests and wishes of their families, and the families were denied of the deceased person's personal belongings (emails and the content of Facebook profile). Furthermore, there could be serious implications for free speech, for media rights, and for keeping accurate historical records.²¹

¹⁷ *Jäggi v. Switzerland*, no. 58757/00, ECHR 2006-X, *Estate of Kresten Filtenborg Mortensen v. Denmark* (dec.), no. 1338/03, ECHR 2006-V, Koch v. Germany no. 497/09, ECHR 19/07/2012.

¹⁸ See *Estate of Kresten Filtenborg Mortensen v. Denmark*, where the Court made a distinction between the cases where the living lodged a complaint for the breach of their privacy in the connection to deceased, as opposed to a deceased person's right to respect for private or family life. The Court concluded: "In the present case the individual in question, namely KFM, was deceased when the alleged violation took place and hence when his estate, on his behalf, lodged the complaint with the Court alleging an interference with his right, or rather his corpse's right, to respect for private life. In such circumstances, the Court is not prepared to conclude that there was interference with KFM's right to respect for private life within the meaning of Article 8 § 1 of the Convention."

¹⁹ J Berg "Grave secrets: Legal and ethical analysis of postmortem confidentiality" (2001) 34 *Connecticut Law Review* 81-122, at 94.

²⁰ as e.g. *In re Ellsworth*, No. 2005-296, 651-DE (Mich. Prob. Ct. 2005), or *In re Request for order requiring Facebook, inc. to produce documents and things*, Case No: C 12-80171 LHK (PSG), 9/20/201, for a commentary see J J Darrow and G Ferrera, "Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?" (2006) 10 *NYU Journal of Legislation & Public Policy* 281-320, at 287.

²¹ See e.g. *Case of Éditions Plon v. France*, no. 58148/00, ECHR 2004-IV.

It is not an ambition of this paper to explore all the possible arguments for protecting post-mortem privacy. Rather, the focus will be, as already emphasised, on the informational privacy of the deceased. Notwithstanding the general arguments above, it is argued here that some form of protection to the deceased person's data should be envisaged. The protection need not be perpetual or all encompassing, and relevant safeguard for the freedom of expression, for historical records and archives, and for legitimate interests of others should be provided. However, freedom of testation and wishes of the deceased should be respected. In the absence of the deceased's wishes, the protection could be achieved through certain default rules in the data protection regimes. This would be a useful addition to protection already provided by copyright, personality rights, or rights to dignity. The paper will further focus on discussing legal options and models for protecting post-mortem privacy through the *Data Protection Regulation*.

3. The current regimes and decedent's data

The protection of post-mortem privacy will now be assessed from the angle of informational privacy and the current state of affairs in this area within the EU.

The *Data Protection Directive* does not mention deceased's data in any context. However, keeping in mind the manoeuvring space in implementation that a directive affords to EU member states²², it has been possible for member states to introduce some kind of a post-mortem protection, even limited in its scope, and for a shorter period of time after death. There are only few examples of member states, which have taken advantage of this possibility.

Bulgaria, for instance, recognises that "in event of death of the natural person his/her rights shall be exercised by his/her heirs",²³ thus extending the right of access to personal data not only to the natural person, but also to his or her family. The Estonian *Data Protection Act* goes even further, giving a considerable amount of freedom to an individual to decide on the use of personal data in the event of processing personal data with the consent of a data subject.²⁴ In s 12 it states: "The consent of a data subject shall be valid during the life of the data subject and thirty years after the death of the data subject, unless the data subject has decided otherwise." Furthermore, in s 13 it entitles certain family members to permit processing of personal data after the death of the data subject, but again for no more than thirty years after death.²⁵

²² See ECJ ruling in *Lindquist* case: „On the other hand, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it.“ Judgment of the European Court of Justice C-101/2001 of 06/11/2003, § 98.

²³ Article 28 (3) *Bulgarian Personal Data Protection Act*, State Gazette No. 1/4.01.2002, 70/10.08.2004, 93/19.10.2004, 43/20.05.2005, 103/23.12.2005, 30/11.04.2006, available in English at: <http://legislationline.org/topics/country/39/topic/3> (accessed 05 Jan 2013).

²⁴ Estonia, *Personal Data Protection Act*, RT I 2003, 26, 158, RT I 2004, 30, 208, available in English at: <http://www.legaltext.ee/text/en/X70030.htm> (accessed 05 Jan 2013)

²⁵ *Ibid*, Article 13(1).

Conversely, the Swedish *Data Protection Act* explicitly refers to personal data of the living, defining personal data as “all kinds of information that directly or indirectly may be referable to a natural person who is alive.”²⁶ Similarly, the UK *Data Protection Act* defines personal data as “data which relate to a living individual”.²⁷ Other member states also predominantly use the term “natural person”; understood generally as a person having legal capacity, starting with the birth and ending with her death.²⁸

Article 29 Working Party, discussing the concept of personal data, maintains that: “Information relating to dead individuals is, therefore, in principle, not to be considered as personal data, subject to the rules of the Directive”.²⁹ However, it also notes that, in certain cases, the deceased’s data could receive some kind of protection. Thus, the controller or processor may not be able to ascertain whether a person is alive or not; protection could be awarded indirectly, since the data could be connected to those of a living person; some legal rules other than data protection could protect the deceased’s personal data (doctor-patient confidentiality, for example). Finally, member states could extend the scope of the national legislation implementing the provisions of *Directive 95/46/EC*, and include protection of some aspects of deceased’s personal data.³⁰ The last option, as demonstrated above, has been used by some member states.

However, most of the EU member states did not utilise the possibility of extending the definitions of personal data and data subjects in their legislation. Furthermore, even the existing legislation is not consistent, and gives only limited protection for the deceased’s data, both in the scope and the length of protection awarded. The legislation is not harmonised and gives different powers to the heirs and data subjects. In sum, in spite of the general possibility of protecting post-mortem privacy through the EU data protection regime(s), this protection is only sporadic and lacks clarity and harmonisation.

4. The revised EU data protection regime

4.1. Definition of personal data and the deceased

Let us now turn to the forthcoming reforms of the EU data protection regime and assess whether it could include protection of post-mortem privacy. The proposal will be looked at from the perspective of the data subject and personal data definitions in order to identify if the regulation generally includes the deceased’s personal data in the scope of the protection it envisages.

²⁶ S 3, Sweden, *Personal Data Protection Act* (1998:204), available in English at: <http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf> (accessed 05 Jan 2013)

²⁷ S 1 (1) (e) *Data Protection Act 1998 c. 29*.

²⁸ Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP 136, at 22.

²⁹ *Ibid.*

³⁰ *Ibid.*, 16, 22, 23.

The European Commission Proposal for the *General Data Protection Regulation* does not mention deceased persons or their data at all. Having in mind a definition of personal data and the data subject, as set in Article 4 of the Proposal, it could be concluded that only living, natural persons' data are within the scope of protection in the Proposal ("data subject' means an identified natural person or a natural person who can be identified..."). Moreover, in the revised version proposed by the Council of the European Union, deceased persons are explicitly excluded as data subjects: "The principles of data protection should not apply to deceased persons."³¹ This amendment has been advocated by the Council representative of Sweden, a country that excludes the deceased's data explicitly, as noted above. If the proposal is adopted in that text, or in one similar, we would have a more disadvantageous situation for the protection of decedents' personal data than the current one described earlier. Provided that the Regulation is adopted in that form and with the aforementioned or similar content, member states would not be entitled to change its text and, hypothetically, award protection to the deceased's personal data.³² The most recent European Parliament Draft Report, however, does not contain this amendment and retains the definition initially proposed by the Commission, with some clarifications that do not consider the deceased's data.³³ There is, apparently, a long way to go before the text is finalised and all the options still seem open. Nevertheless, having seen different proposals so far, the option of explicitly including the deceased's data within the scope of the protection awarded by the new regime appears quite unrealistic.

Conversely, it could be argued that some elements of the proposal could be seen, at least hypothetically, as promoting post-mortem privacy protection. There are certain novelties in the proposals, which could serve as a base for discussing a potential shift in the EU data protection system and a move towards the property-based regime. The first proposal refers to a more general shift towards the *commodification* of personal data and, arguably, a certain departure from the human rights basis for the protection of personal data. The proposals for introducing the right to be forgotten and data portability could also serve to support this argument. Thus, the proposal will be further assessed through the lens of *propertisation* of personal data and its possible, hypothetical, effects on post-mortem privacy.

³¹ Revised Recital 23, Council of the European Union, *Letter from the Presidency to Working Party on Data Protection and Exchange of Information*, 2012/0011 (COD), Brussels, 22 Jun 2012, available at http://amberhawk.typepad.com/files/blog_june2012_eu-council-revised-dp-position.pdf (accessed 05 Jan 2013).

³² See e.g. *Frontini v Ministero delle Finanze*, C - 183 [1974] 2 C.M.L.R. 372 ("...regulations...should not be the subject of state-issued provisions which reproduce them, either in full or in an executory manner, and which could differ from them or subject their entry into force to conditions, even less which take their place, derogate from them or abrogate them, even in part." p 12).

³³ See amendments 14 and 84 in Jan-Philipp Albrecht, a Rapporteur for the European Parliament's Civil Liberties, Justice and Home Affairs Committee, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* 2012/0011(COD) 17.12.2012.

4.2. The Proposal for propertisation of personal data?

4.2.1. General features of property-based data protection

Before assessing the Proposal in the light of the *propertisation* of personal data, it is useful to present the main feature of such a regime. As opposed to the data protection models based on human rights or torts, there is a widely discussed model of property rights in personal data. European countries have mainly perceived privacy and control over personal data as a human right,³⁴ whereas the US has been using a torts model to protect privacy.³⁵ The UK is somewhere in between. The property-based model is merely a theoretical construction, as it has not been applied so far.

The property rights model is based on a presumption that personal data in practice already are, or should be considered, as an asset or commodity. For economists, this debate is less controversial and the value of personal data as a new asset has been recognised. Thus, for instance, the World Economic Forum (WEF) in its 2011 personal data study, referring to personal data as “the new ‘oil’ – a valuable resource of the 21st century”, predicts that “it will emerge as a new asset class touching all aspects of society.”³⁶ The term “asset” in this debate is closely related to the notion of “commodification”, originally a Marxian concept³⁷, but given different meanings by contemporary economic theory. Radin, for example, usefully defines this concept both in a narrow and broad sense. For her, in the narrow sense of the term, “commodification describes actual buying and selling (or legally permitted buying and selling) of something.” On the other hand, broadly, *commodification* includes also “market rhetoric, the practice of thinking about interactions as if they were sale transactions, and market methodology, the use of monetary cost-benefit analysis to judge these interactions.” In addition, the most extreme notion “universal commodification” solves problems of contested commodities (such as bodily parts, blood, or information and personal data) “by making everything in principle a commodity.”³⁸ Under this conception, personal data, especially given its aforementioned market value, could certainly qualify as a commodity and an asset.

³⁴ Article 8 of *The Charter of Fundamental Rights of the European Union*, 2007/C 303/01, or see J E J Prins, “Privacy and Property: European Perspectives and the Commodification of our Identity” in L Guibault and P B Hugenholtz (eds), *The Future of the Public Domain* (The Hague: Kluwer Law International, 2006) 223-257.

³⁵ *Restatement (Second) of Torts* §§ 652A-652E (1977) or A J McClurg, “A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling” (2003) 98 *Northwestern University Law Review* 63-144.

³⁶ World Economic Forum “Personal Data: The Emergence of a New Asset Class” 2001 available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 10 Jan 2013) at 5, 7.

³⁷ K Marx *A contribution to the critique of political economy*, translated from the German by S W Ryazanskaya, edited by M Dobb (Moscow: Progress; London: Lawrence & Wishart, 1971) and vol. 1 part 1 ch 1 in K Marx and F Engels (ed), *Capital; a critique of political economy* (New York: International Publishers 1967).

³⁸ M J Radin, “Market-inalienability” (1986) 100 *Harvard Law Review* 1849-1937, at 1861.

The legal recognition of personal data as an asset is less clear and far more controversial.

The property rights model for the protection of privacy has been debated rather extensively within the US legal and economic scholarship. One of the first advocates of the property model, Westin,³⁹ discussed it as early as 1968. Building on his theory, Laudon proposed “market-based mechanisms based upon individual ownership of personal information and National Information Markets (NIM) where individuals can receive fair compensation for information about themselves.”⁴⁰ Other eminent US legal academics, proposing different variations and adjustments to this model, are: Schwartz,⁴¹ Mell,⁴² Zarsky,⁴³ Lessig,⁴⁴ etc. The arguments that proponents of this system use concentrate around one main goal: enabling individuals to better control the collection, use and transfer of their personal data, and to participate in sharing the profits resulting from the use, and processing of, their personal data. Lessig argues that this model can be supported by the Privacy Enhancing Technologies that enable users “both to encrypt and to express preferences about what personal data is collected by others.”⁴⁵ He argues that privacy should be regulated within the regime of property law so that people could “take ownership of this right, and protect it” like it is the case with copyright.⁴⁶ Along this line, when discussing the model and, in principle, arguing against it, Samuelson detects its two main benefits: an ability of individuals to sell their personal data and recoup some of their value in the market and to force companies to internalise these new costs and make better decisions on investing in the collection and use of personal data.⁴⁷ In addition, since property rights are rights *in rem* and have *erga omnes* effect (can be enforced against anyone), property in personal data could help individuals to protect their rights, not only against data controllers, but against third parties as well, such as, for instance, mirroring websites, which store personal data without either the data subject or the data controller being aware of it.⁴⁸ Also, using the same argument that Conley applied for the US context, Koops finds that an important benefit of the property over the torts

³⁹ A F Westin, *Privacy and freedom* (New York: Atheneum, 1967).

⁴⁰ K C Laudon, “Markets and privacy” (1996) 39 (9) *Communications of the ACM* 92-104, at 96.

⁴¹ P M Schwartz, “Property, privacy, and personal data” (2003) 117 *Harvard Law Review* 2056-2128.

⁴² P Mell, “Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness” (1996) 11 *Berkeley Technology Law Journal* 1-79.

⁴³ T Z Zarsky, “Desperately seeking solutions: using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society” (2004) 56 *Maine Law Review* 13-59.

⁴⁴ L Lessig, *Code, version 2.0* (New York: Basic Books, 2006).

⁴⁵ *Ibid*, 276.

⁴⁶ In Code 2.0 Lessig adds a new model, where P3P negotiates and concludes “contract” with the website. *Ibid*, 229 – 230.

⁴⁷ P Samuelson, “Privacy as intellectual property” (1999) 52 *Stanford Law Review* 1125-1167, at 1128.

⁴⁸ Similarly, B J Koops, “Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice” (2011) 8(3) *SCRIPTed* 229-256.

privacy regime—namely, that there is no need for individuals to demonstrate harm—works well for the European context, too.⁴⁹

There are, nevertheless, notable disadvantages of this model. Litman, for example, forcefully argues that the property model would encourage transactions in personal data, which should, in fact, be discouraged. Also, alienability, as a feature of property, would vest control in the data miner, rather than the individual.⁵⁰ Cohen likewise maintains that property rights in personal data would enable more trade in personal data, and would ultimately result in less privacy.⁵¹ Similarly, Samuelson notes that individuals would not be able to control the further transfer of their personal data, given that free alienability is a “a common, even if not ubiquitous” characteristic of property, which would allow the purchaser of personal data to sell it further and, therefore, lessen the control that that owner initially had.⁵² Furthermore, there are legitimate concerns for an imbalance with freedom of expression that *propertisation* of personal data may create. In this regard, Litman warns that recognising property in personal data would mean recognising property in facts, which are “building blocks of expression; of self-government; and of knowledge itself” and, thus, would entitle the owner to restrict different uses of the fact.⁵³ Along this line of argument, Samuelson finds this regime inappropriate for the protection of personal data, arguing that it effectively creates a new regime of intellectual property in information with completely different purposes and mechanisms than that of the traditional intellectual property system.⁵⁴ Furthermore, if privacy is considered a human right, *propertisation* of personal data could seem unnecessary and even, as Samuelson notes, “morally obnoxious”. She makes a comparison with other civil rights, concluding that, from this perspective, “it may make no more sense to propertize personal data than to commodify voting rights.”⁵⁵

European judiciary and academics mainly refuse to perceive personal data as a commodity, arguing that human rights maintain and reflect personal integrity and liberty, and, therefore, there is no room for a property approach. Consequently, privacy is inseparable from personhood, as a human right cannot be waived or transferred.⁵⁶ However, the issue of transferability of human rights in general is not

⁴⁹ *Ibid*, 247.

⁵⁰ J Litman, “Information privacy/information property” (2000) 52 *Stanford Law Review* 1283-1313, at 1304.

⁵¹ J E Cohen, “Examined Lives: Informational Privacy and the Subject as Object” (2000) 52 *Stanford Law Review* 1373-1426, at 1391.

⁵² P Samuelson, see note 47 above, at 1136.

⁵³ J Litman, see note 50 above, at 1296.

⁵⁴ P Samuelson, see note 47 above, at 1129.

⁵⁵ *Ibid*, 1140, 1141.

⁵⁶ see J E J Prins, see note 34 above, at 234-235 or N Purtova “Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights” (2010) 28 (2) *Netherlands Quarterly of Human Rights* 179-198, or conversely see C Cuijpers, “A private law approach to privacy; mandatory law obliged?” (2007) 24(4) *SCRIPT-ed* 304-318.

very clear and the European Court of Human Rights has recognised the possibility for individuals to waive their human rights, though not in an explicit manner.⁵⁷ Building on this underlying presumption on the possibility to waive a human right, Prins points at the nature of the *Data Protection Directive* provisions, which are in most cases not mandatory, and argues that the current EU regime allows contracting and commercial exploitation of personal data.⁵⁸ Some commentators argue for the opposite. Citing *Mellacher and Others v Austria*, De Schutter, for instance, rejects a possibility of waiving or limiting the right to privacy in any way.⁵⁹ This appears to be the correct position, as the European Court of Human Rights unambiguously declared a non-transferable nature of the right to privacy,⁶⁰ as opposed to a more contested position on transferability of human rights in general.

Nevertheless, Prins goes even a step further, characterising the EU regime as utilitarian, mainly due to the fact that it aims to promote the free flow of personal data. Using this information, as well as recognising the tools of control that are available to individuals pursuant to the Directive, Prins rather controversially argues that the EU regime is more receptive to a property regime than the regime of the US.⁶¹ Similarly, discussing the property model, Purtova argues that it could provide a good framework, which would enable better control of personal data, even within the EU, notwithstanding the differences in property concepts both in common and civil law countries. She argues primarily for introducing the protective features of property, its *erga omnes* effect, rather than its alienability feature.⁶²

⁵⁷ *Deweert/Belgium*, ECHR 27 Feb 1980, A 35 §48-54.

⁵⁸ J E J Prins, see note 34 above, at 243.

⁵⁹ “The right one has to freedom of expression or to respect for private life does not extend to the right to obtain, under the mechanisms of the market, a remuneration for the sacrifice of that right, or even for agreeing to that right being limited in some less complete way.” O De Schutter “Waiver of Rights and State Paternalism under the European Convention on Human Rights” (2000) 51 *The Northern Ireland legal quarterly* 481-508, at 487; see *Mellacher and Others v. Austria*, Application No. 10522/83; 11011/84; 11070/84, Judgement of 19/12/1989 para 506; also N Purtova, see note 56 above, at 16.

⁶⁰ See in this regard the *EC Data Protection Regulation Proposal* see note 9 above, at 2. “The Court confirmed the principle that Article 8 was of a non-transferrable nature and could thus not be pursued by a close relative or other successor of the immediate victim in the cases of *Thevenon v. France* ((dec.), no. 2476/02, 28 June 2006) and *Mitev* (cited above).” para 79 *Koch v Germany*, see note 17 above

⁶¹ *Ibid*, 245.

⁶² “Property, with some limitations resolved by regulation, due to its *erga omnes* effect and fragmentation of property rights, has the potential to reflect and control this complexity of relationships. This may be considered an instance of property exercising its protective rather than market function; it aims at making sure that even after transfer of a fraction of rights, a data subject always retains basic control over his personal information.” N Purtova “Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence” in S Gutwirth et al (eds.), *Computers, Privacy and Data Protection: an Element of Choice* (Springer Science Business Media B.V. 2011) 39-64, at 61.

4.2.2. *Is there a move towards propertisation of personal data in the EU?*

Even if we did not initially agree with arguments put forward by Prins or Purtova about receptiveness of the EU data protection regime towards the property rationale, the proposed framework could provide us with more arguments and indications supporting this viewpoint. The first, interesting and perhaps indicative example is the narrative that points to a move towards the property model of protecting personal data. This move has not been explicitly endorsed, but it can be traced in some European Commission officials' statements.⁶³ These statements may be seen as unintentional, when referring to the property model, but the content of the Data Protection Regulation Proposal certainly indicates this tendency. Apart from this anecdotal argument, the parallel between the property-based data protection regime and the new proposal for a European Regulation can be drawn in relation to the proposal's aim to provide better control of individuals in relation to the collection and use of their personal data.⁶⁴ The aim is compatible with the main goal of property-based regimes, discussed above. Additionally, the proposal strongly aims to promote the free flow of personal data. This is clearly a utilitarian goal, and one of the main reasons for establishing private property regimes in general.⁶⁵ Some authors would go even further and argue that the proposed regime neglects the human rights basis of the data protection regime.⁶⁶

In addition to these general features of the new regime that resemble a property model, further arguments could be traced in two notable innovations of the proposal: the "right to be forgotten" and data portability. The "right to be forgotten" is introduced in the Article 17 of the General Data Protection Regulation Proposal. So far, data subjects have had a right to request deletion of personal data the processing of which does not comply with the provisions of the Directive,⁶⁷ but this right is not as comprehensive as the right to be forgotten. The new right would encompass not only the right to have personal data erased, but also "the abstention from further dissemination of such data."⁶⁸ The right includes a duty of data controllers, who have

⁶³"Our proposal starts from everybody owning their own personal data." N Kroes, Vice-President of the European Commission responsible for the Digital Agenda, EU Data protection reform and Cloud Computing, SPEECH/12/40, 30/01/2012, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en> (accessed 10 Jan 2013).

⁶⁴ See recital 6 and p 2 of *the Data Protection Regulation Proposal*, see note 9 above.

⁶⁵ As stated in recitals 3, 4, 5, 7, 8, 14, 78, 96, 105, 133 and Article 46 of *the Data Protection Regulation Proposal*; for a theoretical perspective see e.g. L C Becker *Property rights: philosophic foundations* (Routledge and Kegan Paul, 1977) at 68-70; V Pareto *Manual of political economy* (Kelley 1971); G S Alexander and E M Peñalver *An Introduction to property theory* (Cambridge: Cambridge University Press 2012) at 14.

⁶⁶ See e.g. Amberhawk Training Limited, Hawktalk, "EU Data Protection Regulation Breaks Explicit Link With "Privacy" and Human Rights" 02 Feb 2012 available at <http://amberhawk.typepad.com/amberhawk/2012/02/eu-data-protection-regulation-breaks-explicit-link-with-privacy-and-human-rights.html> (accessed 10 January 2013).

⁶⁷ Article 12(b) of *the Data Protection Directive*, see note 8 above.

⁶⁸ Article 17 (1) *General Data Protection Regulation Proposal*, see note 9 above.

made the personal data public, to inform third parties of the data subject's request to erase any links to, or copy or replicate that personal data.⁶⁹ The Draft Report has recently significantly reduced the proposed effects of the right to be forgotten, changing its title into “right to erasure and to be forgotten”,⁷⁰ and noting that the Commission’s proposal is not quite realistic. It remains to be seen what the final text will look like, as does the previously mentioned concept of the data subject.

The European Commission’s proposal to include this “right to be forgotten” in the new data protection regime has caused a lot of controversy between privacy opponents and companies.⁷¹ The right to be forgotten, however, will not be explored here in any detail. For the purpose of this paper, it serves as an example of another similarity between the proposal and *propertisation* of personal data. It could be argued that this right resembles the right to destroy, an essential feature of property.⁷² In this regard, Koops is one of the rare scholars, who compared the right to be forgotten to *abusus*, a feature of property (“strongest property stick” - the right to destroy). However, he approaches this comparison with caution, maintaining that, if the right to be forgotten is cast in the form of *abusus*, all other property rights (*usus* and *fructus*) would have to be allocated to individuals. For him, this would be “a bridge or two too far.”⁷³ This is not necessarily correct, given the difference between property concepts and “sticks” that are contained within “bundle of property rights” in the civilian and common law jurisdictions. The common law concept of property appears to be more open-ended and relative, as opposed to the more absolutely defined concept in the civilian countries. Therefore, the common law property could include different rights and objects, and does not need to be equated to the concept of ownership (which would necessarily include all the “sticks”).⁷⁴ Consequently, not all the “sticks” would have to be allocated to individuals in the property-based data protection regime.

⁶⁹ *Ibid*, Article 17 (2).

⁷⁰ *Draft Report*, see note 33 above, amendments 146 and 153.

⁷¹ See e.g. Koops see note 48 above, at 537-539 (discussing issues such as: conflicts of the right to be forgotten and provisions of the Data Retention Directive; issues involving social networks, such as destruction of responsibility between them and users, applying household exemption and the right to be forgotten simultaneously; problems with mirroring etc.); M Masnick, Techdir “Europeans Continue To Push For 'Right To Be Forgotten'; Claim Americans 'Fetishize' Free Speech” 04 Feb 2011 available at <http://www.techdirt.com/articles/20110204/00145312961/europeans-continue-to-push-right-to-be-forgotten-claim-americans-fetishize-free-speech.shtml> (accessed 10 Jan 2013); ENISA (the European Network and Information Security Agency) “Study on Data Collection and Storage in the EU”, 20 Feb 2012, at 52; ENISA “The Right to be Forgotten - Between Expectations and Practice”, 20 November 2012, at 2; Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals*, 00530/12/EN WP 191, at 13, 14; P Fleischer “The Right to Be Forgotten, or How to Edit Your History”, 29 Jan 2012 <http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.html> (accessed 10 January 2013).

⁷² See e.g. L Becker “The Moral Basis of Property Rights” in J. R. Pennock and J. W. Chapman (eds), *Property* (New York: New York University Press, 1980) 187-220, at 190-191.

⁷³ B J Koops, see note 48 above, at 247.

⁷⁴ See e.g. W G Friedmann, *Law in a Changing Society*, 2nd ed. (Harmondsworth, Eng: Penguin, 1972), at 94; or J Ball “The Boundaries of Property Rights in English Law” (2006) 10(3) *Electronic Journal of Comparative Law*, 1-34, at 4.

Another novelty in the proposal is the data subject's right to data portability. Article 18 introduces this right, i.e., to obtain from the controller personal data "undergoing processing" (when data have been collected and processed based on consent or a contract) and transfer those data from one electronic processing system to and into another (e.g. to a social network), without being prevented from doing so by the controller. As a precondition for that, the controller is obliged to provide those data in a structured and commonly used electronic format. The right to data portability is also subject to extensive debates and revisions to the initially proposed text. The European Parliament Draft Report proposes deletion of the whole article 18 and its merging with article 15 (Right of access for the data subject), noting that the right to data portability is "a mere specification of the right to data access and thus diminishing to an extent its initial force."⁷⁵ As noted for the other proposals discussed above, it will be interesting to see the final form and content of this right. It does not however, substantially affect the discussion in this paper. This is due to the fact that in any version provided so far, the right significantly departs from the current regime, which does not contain anything resembling such a right, and adds a significant new value to the data protection regime.⁷⁶ The right to data portability could empower individuals and provide for a better control over their personal data, as they would be able to leave the provider/platform that does not satisfy their privacy requirements, for instance, or just shift to a provider with better services.⁷⁷ Rather than discussing this right in detail, for the purpose of this paper, it is important to note that the features of this right are noticeably reminiscent of transfer of property. However, it is not a lucrative right and its enforcement is not possible post-mortem, for example, to stipulate in a will the transfer of personal data from Facebook to Google+, or to a memorial website. It is not, however, certain whether it would be practically viable to transfer data post-mortem, even if permitted. The value of personal data of the deceased for businesses is questionable and needs further research. Data portability in this context was used merely to further highlight the resemblance of the proposed data protection regime to the property regime, even if not consistently and entirely.

4.2.3. Propertisation of personal data and transmission upon death

In theory, a property regime for the protection of personal data would arguably entail individual's control and entitlement to transfer their personal data, not only in life, but also upon death, whether by testamentary or intestacy means. The reason for that is that transfer, both in life and upon death, has traditionally been considered one of the main features of property.⁷⁸ Consequently, in theory, it would enable a better

⁷⁵ *The EP Draft Report*, see note 33 above, amendment 141.

⁷⁶ See Article 12 of *the Data Protection Directive*.

⁷⁷ Zanfir for instance argues that "data portability is a pillar of a stronger, more effective right to control over the processing of the data subject's personal data, along with the right to be forgotten and the right to modify incorrect or outdated personal information stored in databases." G Zanfir "The right to Data portability in the context of the EU data protection reform" (2012) 2 (3) *International Data Privacy Law*, 149-162, at 161-162.

⁷⁸ E.g. A M Honoré "Ownership" in A. G. Guest (ed), *Oxford essays in jurisprudence, a collaborative work* (London: Oxford University Press, 1961), L Becker in J R Pennock and J W Chapman, see note 72 above, at 107-147; "The essential feature of property is that it has an existence independent of a

protection of post-mortem privacy, as the deceased would be able to decide on the faith of his data.

Essentially, all the property, personal and real, corporeal and incorporeal, (to name but a few kinds), form an inheritance, or the estate of a person, and transmits by the rules of succession to the deceased's heirs. In England, for instance, "a person's estate is the aggregate of all the property to which he is beneficially entitled".⁷⁹ In French law, with the notion of *patrimoine*,⁸⁰ comprising a person's rights and liabilities, all rights and liabilities pass on the heir(s), in a way that they stand in the position of the deceased.⁸¹ The same is valid in Germany.⁸²

Conversely, the liability or torts regimes⁸³ would not entirely persist upon a person's demise. For instance, in some cases in common law jurisdictions, purely personal obligations "die with a person".⁸⁴ This position, however, has been revised in England and most of the personal actions arising from torts would survive, according to the *Law Reform (Miscellaneous Provisions) Act 1934*. Only defamation and the bereavement claim would not persist. As noted above, in French and German law, liabilities do pass on to the heirs, in a way that they stand in the position of the deceased.⁸⁵ Similar to English common law, French law states that strictly personal contracts (either by the agreement of the parties⁸⁶ or the nature of the contract⁸⁷) terminate upon death.⁸⁸ This would be the case with most terms of service online,

particular person: it can be bought and sold, given and received, bequeathed and inherited, pledged or seized to secure debts, acquired (in the olden days) by a husband on marrying its owner." *OBG v Allan* [2007] UKHL 21; [2008] 1 A.C. 1 at 309.

⁷⁹ Sec 3 Wills Act 1837 c. 26, this Act does not extend its effect to Scotland; sec 5 (1) Inheritance Tax Act 1984 c. 51, applicable to England, Scotland, Wales and Northern Island; similarly Succession (Scotland) Act 1964 c. 41 in sec 32 defines estate as property belonging to the deceased at the time of death.

⁸⁰ The place where property and obligations meet, similar to the concept of estate in English law. B Nicholas, *The French law of contract* (2nd ed. Oxford: Clarendon Press; New York: Oxford University Press 1992), at 29, 30.

⁸¹ For more see M L Levillard "France" in D J Hayton, ed, *European succession laws* (2nd ed. Bristol: Jordans 2002) 211-243, at 219.

⁸² K Kuhne et al. "Germany" in Hayton *ibid*, 243-271, at 257.

⁸³ Torts - the term used in English common law; liability, delict in civil law: a civil wrong, causing a damage or harm to another person, either by fault, intention, negligence or imprudence; arts 1382, 1383 Code Civil, sec 823 BGB, or R F V Heuston and R A Buckley., *Salmond and Heuston on the law of torts*, 21st ed. (London: Sweet & Maxwell, 1996), at 8; for a comparative analysis see C Van Dam *European tort law* (Oxford: Oxford University Press, 2007).

⁸⁴ Principle "Actio personalis moritur cum persona" in *Beker v Bolton*, see note 10 above; for the comparison between the US and German perspective, see e.g. H Rosler "Dignitarian Posthumous Personality Rights—An Analysis of US and German Constitutional and Tort Law" (2008) 26 *Berkeley Journal of International Law* 153-205.

⁸⁵ For more see M L Levillard in D. J. Hayton see note 81 above, at 219.

⁸⁶ Code civil art 1122.

⁸⁷ *Ibid* art 1795. 2003.

⁸⁸ Or for more see Nicholas, see note 80 above, at 172.

which explicitly exclude transfer or transmission upon the death of the user's accounts, of the user's data, and of the users' content.⁸⁹ Therefore, torts or contracts regimes do not seem to be favourable to post-mortem privacy protection, assessed in relation to the law of succession. Another argument to support this claim is the European Court of Human rights case law that clearly establishes a non-transferable nature of the human right to privacy.⁹⁰

To conclude, if we accept, from the reasons discussed in the section 4.2.2 of this paper, that the proposed regime silently promotes the idea of property in personal data, this could indicate its suitability for protecting post-mortem privacy, as opposed to torts or contracts regimes. *Propertisation* of personal data would need to produce transmission upon death, by giving an option to individuals to decide what happens to their personal data upon death, in the case of testamentary succession, or by default rules that enable their heirs to decide what happens to their data. However, if adopted as proposed, this provision for the "right to be forgotten", for instance, would enable individuals to control their post-mortem privacy, only if they decide to "be forgotten online" and exercise this right before death. Since the regulation proposal, as currently drafted, would not award protection of personal data to the decedents of the deceased person, it would not allow them to stipulate their wish to be forgotten in a will, or to leave that decision to their heirs. This, on the other hand, would be a logical consequence, if the property rights model been adopted in full.

This paper, however, does not argue that *propertisation* is a good solution for the EU data protection. *Propertisation* has been discussed only insofar as it would enable some form of protection of post-mortem privacy. It is used as an example of how, in theory, this protection could be achieved. Thus, it is not argued herein that *propertisation* is the best approach, as adoption of this solution would open various other issues that probably could not be solved satisfactory in the EU context. Some of these issues have been discussed in the section 4.2.1. As noted therein, *propertisation* could result in less control as it would enable more trade in personal data and vest control in the data controllers, not the data subjects. Also, it would jeopardise freedom of expression and threaten balances that intellectual property attempts to establish, when refusing to *propertise* facts. Finally, it would be contrary to the long established human rights rhetoric and legal practice in the EU, which does not favour the *commodification* narrative. The human rights approach is deemed to be more appealing, as it aims to balance the right to privacy and other human rights, such as freedom of expression, and vest control over personal data primarily in individuals. According to this practice, the new regime would need to comply with the Article 16 of *Treaty on the Functioning of the European Union* (the Lisbon Treaty), which establishes the principle that everyone has the right to the protection of personal data, and with Article 8 of the Charter of Fundamental Rights of the EU.

⁸⁹ E.g. L Edwards and E Harbinja "What Happens to My Facebook Profile When I Die?": Legal Issues Around Transmission of Digital Assets on Death" in B Ford (ed), *Digital Legacy and Interaction: Post-Mortem Issues*, (Springer 2013, *forthcoming*) Available at SSRN: <http://ssrn.com/abstract=2222163> or <http://dx.doi.org/10.2139/ssrn.2222163> (accessed 10 Mar 2013)

⁹⁰ *Koch v Germany*, see note 17 above

5. Conclusion

This paper attempts to initiate the discussion about post-mortem privacy and personal data of the deceased amongst legal scholars. It also notes possible points of controversy within this phenomenon. The paper discussed current and newly proposed data protection regimes in the EU through the lens of post-mortem privacy. It asserted that the existing regime, based on the human rights model, hypothetically enabled the introduction and protection of post-mortem privacy, depending on the individual member state and regulatory choice made. However, this regime also contributed to the fragmentation of the protection, which is not beneficial for users, bearing in mind the global reach and nature of the Internet and social interaction therein. The new regime, as currently drafted, does not seem provide sufficient scope for protection of the deceased's data. On the contrary, some versions of the proposal explicitly exclude the deceased.

However, certain elements of the proposal could be viewed as favourable for post-mortem privacy. The discussion about these elements was purely theoretical and it identified certain similarities of the new regime to the property-based data protection model. This has been illustrated by using examples of the "right to be forgotten" and data portability discussions, and referring to the aims of the proposal and the general discourse of *commodification* of personal data. Bearing in mind features of property, as opposed to the torts and contracts regime (post-mortem transferability, applied with aforementioned jurisdictional caution), the Data Protection Regulation Proposal could perhaps be seen as promoting the protection of deceased's data.

The paper does not suggest that the *propertisation* would be the best choice, especially since the long-established EU tradition of treating protection of personal data exists within the framework of the human right to privacy. It asserts that the human rights approach is better in that it requires adequate balances with the freedom of expression and vests control over personal data in individuals. In addition, within the EU, the *commodification* of personal data is a rhetoric that is generally perceived as unfavourable.

It seems that a viable solution could be including the deceased's data in the scope of the definition of personal data in the proposal, and awarding a time-limited protection, with appropriate safeguards in relation to the other relevant interests (freedom of expression, archives and historical records, etc.). In this way, the regime would continue to operate from a human rights basis, and a limited protection of the deceased's data could be actualised. The paper, nevertheless, does not aim to propose clearly formulated solutions. This is merely a suggestion based on the above discussion. The main goal is to question the options and possibilities for post-mortem privacy, on the basis of the presumption made in section 2, that some kind of protection is, in fact, desirable. Further discussion and more concrete solutions will be offered in the author's forthcoming thesis.