

Post-mortem privacy 2.0: theory, law, and technology

Edina Harbinja

To cite this article: Edina Harbinja (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](https://doi.org/10.1080/13600869.2017.1275116)

To link to this article: <https://doi.org/10.1080/13600869.2017.1275116>



© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 22 Feb 2017.



Submit your article to this journal [↗](#)



Article views: 2220



View Crossmark data [↗](#)



Citing articles: 2 View citing articles [↗](#)

Post-mortem privacy 2.0: theory, law, and technology

Edina Harbinja

School of Law, Criminology and Political Science, University of Hertfordshire, Hatfield, UK

ABSTRACT

This paper builds on the general survey of post-mortem privacy set out in the author's earlier work. The concept of post-mortem privacy is further developed both at a theoretical level (underpinned by theories of autonomy) and a doctrinal level (considering concepts such as testamentary freedom, and the protection of personal data). Finally, the paper looks at some current developments of technology (tech solutions for the protection of post-mortem privacy) and law/policy (work done by the US Uniform Law Commission on the Uniform Fiduciary Access to Digital Assets Act – UFADAA). The argument is that both of these regulatory modalities provide examples and illustrations of how post-mortem privacy can be recognised practically, especially in the online environment. The paper is, therefore, setting the scene further in this under-explored area, also aiming to set the basis for the author's subsequent empirical research (attitudes towards post-mortem privacy, quantitative and qualitative).

KEYWORDS

post-mortem privacy; digital assets; deceased's data

1. Introduction

This paper further develops findings set out in the author's earlier work, co-authored with Edwards (Edwards and Harbinja 2013a; Harbinja 2013). The first paper on post-mortem privacy provides a definition of the phenomenon, that is, 'the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after death' (Edwards and Harbinja 2013a, 103). This notion has so far received little attention in law, especially in the common law countries. The authors argue that the new circumstances of the digital world, and in particular the emergence of a new and voluminous array of 'digital assets' created, hosted and shared on intermediary platforms, and often revealing personal or sensitive personal data, require a revisiting of this stance.¹ An analysis of comparative common and civilian law institutions, focusing on personality rights, defamation, moral rights and freedom of testation, confirms that there is little support for post-mortem privacy in common law. Conversely, personality rights, in general, attract greater protection in civilian law, including their survival after death. The authors also find that primary role taken by contract regulation may still mean that users of US-based intermediary platforms, wherever they are based, are deprived of post-mortem privacy rights. Having

CONTACT Edina Harbinja  e.harbinja2@herts.ac.uk

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

established a crucial gap in the online legal privacy protection, the authors suggest that future protection may need to come from legislation, contract or ‘code’ solutions, of which the first emergent into the market is Google Inactive Account Manager (IAM).²

Scholarship in this field is still emerging. Post-mortem privacy is a recognised phenomenon in disciplines such as psychology, counselling, anthropology and other humanities and social sciences. The notion, however, received little if any attention by legal scholarship. Most of the scholarship discusses post-mortem privacy only briefly when analysing legal aspects of digital assets and death in general, or in the context of data protection (Atwater 2006; Darrow and Ferrera 2006; Desai 2008; Cahn 2011; Mazzone 2012; Beyer and Cahn 2013; Hackett and Connolly 2013; Hopkins 2013; McCallig 2013, 2014; Lee 2015). The scholarship mainly originates from the US, usually offers some practical solutions (both legal and technological ones), and analyses current and emerging legislation (e.g. Conner 2010–2011; Perrone 2012/2013; Beyer and Cahn 2013; Sherry 2013). It does not, however, conceptualise the notion of post-mortem privacy, nor does it offer solid support and coherent arguments for a more comprehensive legal recognition of post-mortem privacy.

This paper, therefore, aims to address the gap and conceptualise the phenomenon further. Following the earlier research conducted by the author, the focus herein is also on the digital post-mortem privacy, that is, privacy of the deceased Internet user. The same rationale for the choice of this focus is applicable here, that is, the circumstances of the digital world, and the emergence of a new and voluminous variety of ‘digital assets’ that include an unprecedented amount of personal data, merit a fresh perspective of post-mortem privacy. In Section 2 of this paper, the concept will be developed at a theoretical level, underpinned by theories of autonomy established in the works of Bentham (1843), Locke (1947), Mill (1984), Kant (1991), Hegel (1967), Raz (1986) and Rawls (1999). These theories further translate into theories of privacy as an aspect of autonomy, which the author adopts and uses in conceptualising post-mortem privacy. Further support for the recognition of post-mortem privacy is sought in the concept of testamentary freedom, that is, the extension of autonomy post-mortem with regards to the disposition of one’s property. In Section 3 the paper moves to a doctrinal discussion, looking at the current, piecemeal protection of post-mortem privacy through some other legal concepts (e.g. personality rights, data protection), and explores recent regulation in the US, which impliedly recognises this phenomenon (work done by the US Uniform Law Commission (ULC) on the Uniform Fiduciary Access to Digital Assets Act – UFADAA, as revised in late 2015). This section also looks at current developments of technology, that is, tech solutions for the protection of post-mortem privacy (e.g. Google IAM and Facebook Legacy Contact). It could be argued that these novel technological and policy developments demonstrate the growth of popularity of an active post-mortem privacy convention even in US common law jurisdictions, which have traditionally been more opposed to the concept. It is worth noting, however, that the paper does not consider jurisdiction per se, as jurisdiction does not play a vital role in the conceptualisation of the phenomenon in this instance.

2. Autonomy, testamentary freedom and post-mortem privacy

There are various stakeholders relevant to the issues surrounding post-mortem privacy online, viz. Internet users, families, service providers, friends and society. The author

takes a normative stance and promotes the interests of the users over their family or intermediaries. The reason for this is that autonomy is asserted herein as the key value driving the development of the law in this area. Simultaneously, there is a clear drive in the market to provide such autonomy via Google IAM or Facebook Legacy Contact. Furthermore, the US ULC work in the area illustrates a significant policy drive towards a greater recognition of post-mortem privacy.

The following section will first briefly look at the most significant theories of autonomy. These theories will be subsequently discussed in relation to the conceptions of privacy, with the main aim to restate the link between the two concepts and then relate it to the notion of post-mortem privacy. It is argued here that autonomy should be further extended on death, *inter alia* in the form of post-mortem privacy. The analogy drawn to support this argument is that of testamentary freedom, as another concept that implies the extension of an individual's autonomy on death, by way of disposing of his property through a will.

2.1. A brief conceptualisation of autonomy

Autonomy as a concept is difficult to define, and it takes various meanings and conceptions, based on different philosophical, ethical, legal and other theories.³ The theories of autonomy draw both from deist and atheist ethical stances, will and interest theories of rights, natural law and its opposition, explaining autonomy in relation to liberty, dignity, self-realisation, social contract, public interest and moral (Schneewind 1998). The aim of this section is to look at the conceptions of autonomy briefly and to the extent that this discussion can subsequently be utilised in the privacy and post-mortem privacy analysis.

Most classical thinkers explore autonomy, relating it to freedom, ethics, personhood, dignity and other values. The focus of this paper is on personal autonomy and not on 'moral autonomy', as used in Kant's work and Kantian scholarship. However, it is still necessary to refer to Kant's theory first, as his discussion of autonomy is one of the most comprehensive and influential of all times (Schneewind 1998, 550–555).

Kantian autonomy is closely linked to ethics and represents the revolutionary thinking of morality in the eighteenth century. His theory is still extremely influential and provides a focal point for the contemporary scholars' discussions on ethics as well (Schneewind 1998, 3–11). Kant's morality is based on self-governance and autonomy. According to Kant, human beings are rational, autonomous, self-governing and they legislate moral law (Kant 2003, 31.10, 25.14). This action by their will is a pre-condition to their obedience of the moral law. In his later work, Kant refines his theory and introduces two principles. The first principle mandates that human beings act externally only to allow 'the freedom of the will of each to coexist together with the freedom of everyone in accordance with a universal law'. (1991, 6.230, 56). The second principle means that we are to 'act according to a maxim of *ends* which it can be a universal law for everyone to have' and these ends are our perfection and happiness of others. This principle is also known as Kant's categorical imperative (1991, 6.395, 198). Kant believes that acts to which someone has a right may be obtained by compulsion, whereas the adoption of ends and virtue must result from free choice (1991, 6.381, 186).

Locke, like Kant, engages in contemplating morals and free will. According to him, the will is the power or deciding on an action, and our will engages only when we think there

is good or bad at stake (1979, II.XXI. 31–38, 250–256). Willing to him is ‘preferring an Action to its absence’ (Locke 1979, II.XXI. 21, 244). Bentham also talks about will and autonomy in the context of his utilitarian writing on the greatest happiness principle. According to Bentham, we must overcome a divergence between duty and interest by our action. This means that we will pursue morally proper goal if legislation makes it clear that it is to our interest (1948, X.5–7, 10; VII.1.).

Certain theories of property also refer to autonomy and free will in their attempt to justify the concept of property. Hegel, for instance, understands property as an extension of personality and one’s free will (1967, 169–186). For him, the property is ‘the relation of personality to the external sphere of things, understood in terms of the free will’ (Penner 1997, 173). Also, ‘A person must translate his freedom into an external sphere in order to exist as an idea.’ (Hegel 1967, 41). Further, free will in every stage of development is embodied in something, externalised, and since things have no will, there is an absolute right of appropriation. Therefore, a person with a will has a right to appropriate and determine the use of a thing which is considered as not having the will (Penner 1997, 174; Alexander and Peñalver 2012, 59–61). Similarly, Radin classifies property as fungible and personal, arguing that property is an essential vehicle for the development of personality (1982, 957). Radin bases these arguments on the notion of the autonomous self and individual development, that is, autonomy (Alexander and Peñalver 2012, 69).

Many contemporary legal scholars use the notion of autonomy based on the classical concept of liberty (Safranek and Safranek 1998, 738; Bernal 2014, 30). An extremely individualistic stance taken by John Stuart Mill (1984, 72) in his classical work *On Liberty* has been followed by Raz and Rawls, who place the emphasis on an individual as an author of his own life, including a degree of control and leading to happiness and good life (Raz 1986, 369; Rawls and Freeman 1999, 365). For Raz, an autonomous person is one who ‘is a (part) author of his own life’ (1986, 369) and autonomy is a ‘constituent element of the good life’ (1986, 408).

In summary, with all the differences in their approaches and the line of arguments, a great number of classical and contemporary western philosophers and social theorists consider autonomy as one of the central values and basis of their ethical and social theories. This paper builds on the literature and further explores the relationship between autonomy and privacy, to justify its normative stance. The conceptions of autonomy used to underpin the arguments of this paper are those of personal autonomy as explained in the works of Hegel (1967), Mill (1984), Bentham (1843), Raz (1986), Rawls (1999) and Rao (2000). The article does not draw from the ethical considerations of autonomy, as suggested by Kant (1991). The reason for this is that in the author’s view, focusing on the individual autonomy is a first necessary step in identifying the initial scope of post-mortem privacy as a phenomenon, which could be subsequently limited by the conflicting interests of the public (e.g. free speech, historical records and archives, etc.).

2.2. Autonomy and privacy

Many Western authors consider autonomy and privacy inseparable and include autonomy as substantiated in the section above in their conceptions and definitions of privacy. Ortiz, for instance, argues that privacy defines ‘the scope and limits of individual autonomy’ and links privacy to property (Ortiz 1988, 92). For him, property includes autonomy as

dominion over things and physical sphere, whereas privacy represents dominion over oneself (92). Similar view has been offered by Henkin (1974, 1425). This stance closely related to Hegel's theory and Radin's theory of property and personhood mentioned in the above section. There is a rich scholarship on privacy, autonomy, dignity and personhood that makes similar links and interrelations.⁴ Recent UK privacy scholarship follows the similar line of arguments as well. Bernal, for instance, maintains that 'privacy is a crucial protector of autonomy' (2014, 9). Bernal bases his approach on Raz's and Rawls's conceptions of autonomy, mentioned in the previous section.

Some of the most prominent US privacy theorists, such as Nissenbaum (2010) and Solove (2007), also discuss the relationship between privacy and autonomy, setting the discussion in the digital environment. For Nissenbaum, privacy is an aspect of autonomy over one's personal and privacy which frees us from the 'stultifying effects of scrutiny and approbation (or disapprobation)', contributing to an environment that supports the 'development and exercise of autonomy and freedom in thought and action' (83). Nissenbaum further asserts that privacy is essential for our ability to make effective choices and to follow them through, which is an essential aspect of autonomy understood as explained earlier (2010, 82–83). Eventually, therefore, privacy is about control, as much as autonomy and property are (Bernal 2014, 35). Similarly, an even more radical privacy as negative liberty stance is taken by Rosen (2001, 166).

Cohen, on the other hand, offers a critique of this liberal conception of the autonomous self, noting the post-modernist critique of social constructivism and calling for a more nuanced theoretical account of privacy 'in a world where social shaping is everywhere and liberty is always a matter of degree'. (2012, 7). Schwartz belongs to the group of scholars who see privacy in the positive liberty manner, arguing that there should be constraints to day to day autonomy and privacy so that one's capabilities can be developed and make better long-term choices (1999, 1660–1662). This is known as a 'constitutive privacy' school of thought, which recognises autonomy as the core of privacy, but also requires external enablement and protection, because of the societal influences on the core of the autonomous self (Allen 1999; Cohen 2000). In addition, there are scholars who put communitarian interest, welfare and security before the individual autonomy and privacy, putting forward the arguments such as privacy as commons (Etzioni 2000; Posner 2008). Regan (1995), Rao (2000) and Bennett and Raab (2006) argue that privacy promotes equality, while Solove maintains that privacy serves multiple both individual and collective purposes, which are bound up with everyday experience.

Based on the conceptions of privacy as an aspect of autonomy, Bernal has recently proposed the concept of internet privacy rights, restating their grounding in autonomy (2014). His conception of the internet privacy rights essentially regards the concept of informational privacy, which is arguably the most significant aspect of privacy online. This paper adopts his conception and develops it further with regards to post-mortem privacy.

2.3. Testamentary freedom and post-mortem privacy

The conception of post-mortem privacy developed in this paper means that autonomy should in principle transcend death, allowing individuals to control their privacy/identity/personal data post-mortem, analogous to their post-mortem control of property through the concept of testamentary freedom.

In comparative academic discussions on succession laws, it is common knowledge that the freedom of testation as a concept is much more limited in the civilian systems than it is in common law countries. The practically unlimited freedom of testation is considered inviolable in common law,⁵ stemming from liberal, *laissez-faire* economic and social thought revolving around liberty and autonomy, which were explored in the section above (du Toit 2000, 360; De Waal 2007, 14). Examples of thinkers who explicitly supported freedom of testation include Bentham, Mill, and Locke.⁶ Blackstone, for instance, maintains that wills are ‘necessary for the peace of society’ and testamentary freedom is a ‘principle of liberty’ (1829, 437–438). It has been said that testamentary freedom ‘crystallised eighteenth-century liberal thinking in relation to property’ and was seen as ‘a means of self-fulfilment’ (Atherton 1988, 134). Case law has developed similar stances. For instance, Cockburn C J observed in the 1870 case of *Banks v Goodfellow*: ‘The law of every civilised people concedes to the owner of property the right of determining by his last will, either in whole or in part, to whom the effects, which he leaves behind him shall pass.’ In civilian countries, this principle is considerably limited by the notion of forced heirship, giving certain family members indefeasible claims to a part of the testator’s estate. Justifications for limiting the principle of testamentary freedom originate from ethical, philosophical and natural law thoughts, arguing for ‘solidarity between generations’ (De Waal 2007, 15).

Looking at freedom of testation from another perspective, more individual and personal, some authors argue that the freedom of testation is an aspect of the testator’s personality rights. As such, it cannot be detached from an individual, delegated or transferred from another person (Sonnekus 2007, 79). Similarly, others characterise the freedom of testation as the manifestation of autonomy, having a considerable effect on the emancipation of the individual (Friedman 1966, 355; De Waal 2007, 169). Therefore, if we share these views and see freedom of testation as another personality right, it could seem somewhat odd that countries which provide more protection for personality rights in general, restrict the freedom of testation more (e.g. Germany), whereas countries that, arguably, provide less protection for personality rights (e.g. the UK and US states) value and protect freedom of testation more (Edwards and Harbinja 2013a). This could only bring us back to the economic and market rationale in explaining the ‘unlimited freedom of testation’ in common law countries, giving a little space for personality arguments. Along the same line, civilian countries limit freedom of testation for similar reasons, economic and social, putting personality rights arguments behind.

Freedom of testation has been briefly analysed herein in order to relate this general concept to post-mortem autonomy and post-mortem privacy. The section, however, did not include many details about the laws surrounding the freedom of testation, as the conceptual comparisons were the focus of the section. The argument proposed in this paper is that freedom of testation should translate into the online environment, where digital assets mainly comprise of informational and personal data content (Edwards and Harbinja 2013a, 2013b; Harbinja 2016). These assets are a counterpart of the offline assets and wealth. Therefore, an individual should be able to exercise his autonomy online and decide what happens to their assets and privacy on death. As Bentham puts it in his description of ‘auto-icon’: ‘Every man is his best biographer’ (Naffine 2000).

One of the most obvious objections to extending privacy post-mortem (where it has not already been extended, as found by Edwards and Harbinja 2013a) is that the legal life terminates on death and legal personality ceases to exist.⁷ Legal personality, however, as

found by Naffine, is relative and varies from a branch of law to branch of law and from legal family to legal family. We are particularly interested in the legal personality of individuals for the purpose of this paper (i.e. natural persons), as opposed to that of the companies and other entities that have legal capacity. There is no clear-cut answer as to when the legal personality dies (Tur 1987, 122; Naffine 2000). Legal personality in some cases, such as the testamentary freedom, does extend on death, even impliedly by allowing a deceased person to control their wealth by the wishes they expressed premortem. Along these lines, Simes observes that

though death eliminates a man from the legal congeries of rights and duties, this does not mean that his control, as a fact, over the devolution of his property has ceased. A legal person he may not be, but the law still permits his dead hand to control. (1955, 1)

Tur (1987, 123) is even more critical of the definition of legal personality and its ending on death, arguing

We do not even have ... any clear idea of when a legal person comes into being or when he ceases to exist ... Nor should we regard physical death as marking the termination of legal life, if for no other reason than the existence of a legal will, through which the physically dead person seeks to control the disposition of his property.

This argument can further be related back to Hegel's and Radin's personhood theories of property. Thus, if property is an extension of an individual's personhood and a necessary pre-condition for its development, then this personhood transcends death same way his property does, through a will. Moral rights provide further support for this argument. As a personal aspect of copyright, moral rights extend on the death of a creator, perpetually (e.g. France), as long as the economic rights last, or for a lesser period with an option of waiving these rights (e.g. the UK and the US, Edwards and Harbinja 2013a). This evidence again supports a proposition that aspects of personality, in this case, dignity, integrity and autonomy, do survive death, sometimes even for an unlimited period, as in France. Therefore, legal personality does extend beyond death and so should privacy.

3. Law, technology, and post-mortem privacy

3.1. Piecemeal protection of aspects of post-mortem privacy

As noted earlier, post-mortem privacy is a new phenomenon in legal scholarship and, therefore, this paper will discuss it from a doctrinal point of view as well. This will enable a holistic conceptualisation of post-mortem privacy, encompassing its theoretical underpinnings (i.e. autonomy) and doctrinal arguments (e.g. the protection of personal data) for its legal recognition.

It is worth noting at the outset that one of the most significant arguments against the legal recognition of post-mortem privacy is the lack of real harm to the user, that is, the deceased cannot be harmed or hurt (Beverley-Smith 2002, 124). The analysis in the following sections rejects this argument and makes an analogy with the option to bequeath one's property. Following a similar line of arguments, the deceased should not be interested in deciding what happens to their property on death as they would not be present to be harmed by the allocation. The interests advanced in these cases are not only those of the family and society in the distribution of wealth as freedom of testation

is upheld to a lesser or greater degree in most systems, even where not congruent with the interests or desires of heirs or society. It is submitted here that users do have interests in what happens after their death, in the digital realm this interest is greater than in the offline world, due to the prominence and volume of personal data disclosed online, and the importance of digital assets in creating one's online identity (Edwards and Harbinja 2013b, 115–144). Therefore, similar notions to testamentary freedom in relation to real world property should be developed in online environments, for digital assets and personal data therein.

Research demonstrates that the US and UK laws do not protect post-mortem privacy as such. Protection to some aspects of the phenomenon has been awarded by different legal institutions, such as the laws of privacy, breach of confidence, intellectual property, personality, publicity, defamation, succession, executry and trusts and data protection. This protection is, however, more prominent and encompassing in civil law countries, aiming to protect the values such as autonomy, dignity and reputation, especially of the creators (121). In English and the US common law systems, the principle has traditionally been *actio personalis moritur cum persona*, meaning personal causes of action die with the person, (e.g. defamation claims, breach of confidence claims, wrongful dismissal claims, etc., see *Baker v. Bolton*, 1808). This principle has been revised by legislation mainly in many contexts for reasons of social policy.⁸

It is clear that post-mortem privacy is not protected as such in English law (Edwards and Harbinja 2013a, 125). Although in principle, the same could be said for the US,⁹ some traces of post-mortem privacy protection could be found in individual states' law. According to the Restatement (Second) of Torts, there can be no cause of action for invasion of privacy of a decedent, except 'appropriation of one's name or likeness'.¹⁰ Some states do provide for the protection of so-called 'publicity rights' (rights that usually protect, celebrities, but sometimes all the individuals' right to name, image, likeness, etc.) post-mortem, up to the limit of 70 years after death.¹¹

Protection of personal data is to be found in the rules on data protection in the EU. Do data protection rights survive? Human rights apply only to living persons,¹² and the EU Data Protection Directive 1995 applies only to living individuals as well, protecting the personal data of 'natural persons' (Article 2). However, the Directive leaves discretion in implementation to EU member states to extend this minimum protection, which is guaranteed.¹³ Some EU states have used this possibility, and their data protection laws offer some kind of post-mortem data protection, limited in its scope and post-mortem duration (Edwards and Harbinja 2013a, 131–132). McCallig finds that 12 states protect the deceased's personal data (Bulgaria, Czech Republic, Denmark, Estonia, France, Italy, Latvia, Lithuania, Portugal, Slovakia, Slovenia and Spain); 4 states expressly exclude the deceased (Cyprus, Ireland, Sweden and the United Kingdom); 10 states refer to personal data of a natural person (Czech Republic, Denmark, France, Italy (both natural and legal person), Latvia, Lithuania, Portugal, Slovakia, Slovenia and Spain) and one state provides a temporal limit for protection of the deceased's personal data (Estonia, 30 years on consent, McCallig 2014). The rationale behind not giving protection to the deceased's personal data is the lack of the ability to consent to the processing of data.¹⁴ Similarly to the arguments put forward by Edwards and Harbinja, McCallig also argues that there is no bar in data protection of the Article 8 of the European Convention of Human Rights in recognising the deceased as data subjects (2014). The UK Data Protection Act 1998 defines personal

data as 'data which relate to a living individual' (Data Protection Act 1998, s (1)(e)), denying any post-mortem rights. The new EU data protection legislation, the General Data Protection Regulation, excludes the data of deceased people from the scope of its protection, but also provides an option for member states to recognise post-mortem privacy as well.¹⁵ Given the previous experience, it is unlikely that many of them will use this opportunity and provide the protection.

3.2. Recent developments in the protection of post-mortem privacy in the US

US states have been pioneers in legislating in the area of the transmission of digital assets on death and post-mortem privacy, more generally (J Lamm – 'February 2013 List of State Laws and Proposals Regarding Fiduciary Access to Digital Property During Incapacity or After Death', *Digital Passing Blog* 13 February 2013). These attempts have, however, created very different and ad hoc solutions between the states, resulting in legal uncertainty and jurisdiction issues. The answer to this piecemeal legislation and possible conflicts of law has been an attempt to harmonise the legislation within the US. In July 2012 the US ULC formed the Committee on Fiduciary Access to Digital Assets. The goal of the Committee was to draft an act and/or amendments to ULC acts (the Uniform Probate Code, the Uniform Trust Code, the Uniform Guardianship and Protective Proceedings Act, and the Uniform Power of Attorney Act) that would authorise fiduciaries to manage and distribute, copy or delete, and access digital assets. Starting from 2012, for the purposes of Committee meetings, The Fiduciary Access to Digital Assets Act has been drafted and published online on multiple occasions. (National Conference of Commissioners on Uniform State Laws, 2013). The draft from July 2014 aimed to authorise fiduciaries' to access, manage, distribute, copy or delete digital assets and accounts. It addresses four different types of fiduciaries: personal representatives of decedents' estates, conservators for protected persons, agents acting under a power of attorney and trustees.

The initiative aimed to improve and develop the existing statutes attempting to consider the full range of digital assets.¹⁶ The Committee struggled initially to find adequate solutions to some very important issues in the area. For instance, in the Prefatory Note for the Drafting Committee in the February 2013 Draft, the drafters identified the most important issues to be clarified, including the definition of digital property (Section 2) and the type and nature of control that can be exercised by a fiduciary (Section 4). It seemed that some of the most controversial issues were being disputed within the Committee, such as clarifying possible conflicts between contract and executry law, and between heirs, family and friends.

The following version of the proposal, however, provided for fiduciaries access to all communications, including email contents and log information (unless prohibited by the decedent's will), even in cases where this access conflicts with the ToS (e.g. as seen in Yahoo!'s or Microsoft's ToS above). In these cases, the legislation adopted under the Act would trump ToS.¹⁷ The deceased would be able to control this access by signing a separate set of terms and conditions provided by the service providers.

Additionally, this new draft abandoned the digital property notion altogether and left only the concept of digital assets, comprising both the content and the log information (information about an electronic communication, the date and time a message has

been sent, recipient email address, etc., s. 2 (7) (8)). This draft was adopted by the ULC in July 2014, and a consensus seemed to have been achieved on its text. However, after a further round of lobbying caused by the industry's dissatisfaction with the draft, and resulted in a new version of the UFADAA, adopted in December 2015 (J Lamm, 'Revised Uniform Fiduciary Access to Digital Assets Act' (Digital Passing, 29 Sep 2015) <http://www.digitalpassing.com/2015/09/29/revised-uniform-fiduciary-access-digital-assets-act/>). This draft retains a similar definition of digital assets to that in the previous draft of the Act (Section 2(10), 2015). The biggest difference between the two texts is in recognition of post-mortem privacy and technological solutions analysed in this paper (Google IAM and Facebook Legacy Contact). The Act grants priority to service providers' terms or service and user choices over any other provisions, including the will (Section 4).

The final draft is, therefore, quite revolutionary and supports the main arguments in this paper and those expressed in the author's earlier work, viz. post-mortem privacy and code-law solution for the transmission of digital assets. It will be interesting to see whether the Act will achieve a wider adoption and application in the individual states, or even initiate efforts in other countries.

3.3. Code solutions for post-mortem privacy

Building upon the theoretical and doctrinal analysis in previous sections, this section will evaluate current developments in technology, that is, tech solutions for the protection of post-mortem privacy (e.g. Google IAM, <https://support.google.com/accounts/answer/3036546?hl=en> or Facebook Legacy Contact, <https://www.facebook.com/help/1568013990080948>). These solutions practically recognise and promote post-mortem privacy, giving further support to the concept.

Google has fairly recently launched a pioneering 'code' solution for post-mortem transmission of emails and some other services. The 'Inactive Account Manager', introduced in April 2013, enables users to share 'parts of their account data or to notify someone if they've been inactive for a certain period of time' (Google, Account Help, 'Inactive Account Manager for trusted contacts' <https://support.google.com/accounts/answer/3036514?hl=en>). According to the procedure, the user can nominate trusted contacts to receive data if the user has been inactive for the time chosen by him (3–18 months). The trusted contacts are after their identity has been verified, entitled to download data the user left them. The user can also decide only to notify these contacts of the inactivity and to have all his data deleted. There is a link directly from the user's account settings (data tools section) to the IAM.

A key problem with IAM is verification of trusted contacts. Text messages are sent to trusted contacts (mandatory), and also, the user can choose to be notified of his timeout by email. This could prove problematic as the phone number is not an official way of proving identity. Furthermore, people tend to change their mobile phone providers and numbers, and some of them may never be able to get notified, and the user's wish will not be honoured in these cases. This problem has been recognised by Google, too, but the company considers the two-factor authentication suitable for the time being before better ways of identification are employed (identify tokens, fingerprint identification, etc.).

A second problem is a transfer of content via IAM to trusted contacts, which would provide for different beneficiaries than the offline ones. It would, perhaps, include

friends and digital community that would not be taken into account in an offline distribution of property. This further leads us to the connected problem of conflicts between the interests of the deceased (expressed in his digital will, or traditional will), family (as his heirs) and friends (with whom the deceased might have firmer ties online than those with his heirs offline, as research suggests; Kasket 2013, 7). This issue becomes more complex in different jurisdictions, where Google's users are based in different parts of the world. Google, however, consider themselves bound primarily by the Californian probate law in this and other similar cases (e.g. requesting the US court order in the access procedure described earlier). This is understandable to an extent, especially as the service had been most likely designed and developed initially by the developers and *techies* (staff working on the development of technology mainly), without major input from the legal and policy departments. These inputs probably came at a later stage and Google is still contemplating the viability and scalability of the service. Overall, this could be welcomed as a good development that respects autonomy and allows users much more control over what happens to their data on death. This is especially important as Google stores an enormous amount of user's data, with all the services it provides (Gmail, Youtube, Google+, Google Drive, Photos, etc.).

Facebook seem to have followed Google's lead and IAM with their recently announced option of 'Legacy Contact'. From February 2015, Facebook allows their US users to designate a friend or family member to be their Facebook estate executor and manage their account after they have died. The Legacy Contact has a limited number of options: to write a post to display at the top of the memorialised Timeline; to respond to new friend requests and to update the profile picture and cover photo of a deceased user. In addition, a user 'may give their legacy contact permission to download an archive of the photos, posts and profile information they shared on Facebook'. The Legacy Contact will not be able to log in into the account or see the private messages of the deceased. All the other settings will remain the same as before memorialisation of the account. Finally, an option is that a user decides that their account is permanently deleted after their death. The rationale behind this feature, according to Facebook, is to support both the grieving individuals (it is not clear whether family, friends or all of them) and the users who want to take more control over what happens to their account on death (Facebook 'Adding a Legacy Contact' *Newsroom*, 12 February 2015. <http://newsroom.fb.com/news/2015/02/adding-a-legacy-contact/>).

This move from Facebook is, admittedly, a welcome development for users. It does shift the balance of interests from family and next of kin to users. Users now have control over who their Legacy Contact is, and this can only be one of their Facebook friends. The Legacy Contact does not take too much control over the deceased's account, as they cannot post on behalf of the user (apart from the one message in remembrance and changing the timeline and profile picture) and they need permission to download an archive of the deceased user's content. It is, however, unclear whether this permission includes all the content or some categories. Also, one of the issues is the obscure place of this option (as seen with other options in relation to the deceased's account, see discussion above). To designate a Facebook Legacy Contact, a user needs to go into 'Settings', choose 'Security', and then choose 'Legacy Contact' at the bottom of the page. More importantly, it is unclear whether this option will trump the options heirs and next of kin have according to the existing policy (deactivation and memorialisation as set out above). Facebook

need to make this clear in their terms of service. Also, there might be issues with conflicting interests of heirs/families with a friend designated as a legacy contact and having the option to download the archive of the deceased's content. For instance, if the heirs inherit copyright in the user's works, and the Legacy Contact has acquired this content with the permission of the user, will this content be exempt from the provisions of the will/intestacy laws. With this option, Facebook shifts the balance and accounts more for the deceased's interests and decisions made before death. However, the balance remains unclear, and all this needs to be clarified before Facebook moves to introduce this option to the rest of their user base. Otherwise, a welcome move might end up in a series of legal issues and disputes (Facebook 'Adding a Legacy Contact' *Newsroom*, 12 February 2015 <http://newsroom.fb.com/news/2015/02/adding-a-legacy-contact/>).

In summary, both the services analysed above provide for a post-mortem privacy friendly options for users' control of their digital content and personal data. This is in line with Bernal's conception of internet privacy rights and the individual's right to request deletion of their personal data, extended post-mortem as suggested in this paper. The novel technological developments demonstrate the emergence of an active post-mortem privacy convention even in US common law jurisdictions, which have traditionally been more opposed to the concept of post-mortem privacy.

4. Conclusion

The paper discusses theoretical, doctrinal and technological arguments for the recognition of post-mortem privacy in law and policy. The analysis reviewed the role of autonomy as a value and then discussed how it supports privacy. The author follows the pro-autonomy stance of Nissenbaum (2010) and Bernal's (2014) as justification for the difficult choices herein in favour of users rights, rather than platforms or families.

It is clear the law typically recognises a person's autonomy and as a connected phenomenon, that person's right and ability to dispose of his or her wealth and property. This, however, has arguably not been translated to the online world. As shown in some of the author's earlier works, a user's rights of ownership over digital assets, nor their rights to allocate these assets after death, are routinely recognised (Edwards and Harbinja 2013b; Harbinja 2016). It can be argued that in the online world, digital assets and identities are more closely related to privacy interests than in the offline world, and thus are much more closely related to the personal and autonomy interests of the user. It is therefore argued here that separate from the general consideration of property status and, thus transmissibility; testamentary freedom should in principle extend to digital assets created in the online world.

The author argues for recognition of at least some degree of post-mortem privacy and the right of an individual to dispose of/control their personal data post-mortem. Evidently, like all user interests, post-mortem privacy rights needs to be balanced with other considerations, including the same privacy interests of others and the social and personal interests in free speech and security, etc. It is, unfortunately, not possible in the scope of this paper to analyse the potential exceptions more in detail. The aim of the paper is mere to discuss doctrinal and theoretical grounds for recognising post-mortem privacy. In addition, the paper uses examples from the recent technological and legal developments that do recognise post-mortem privacy implicitly, without using the term as

such. In discussing this difficult and grey question, this paper will take the view that autonomy interests play a vital part, and furthermore, that a framework for recognition of post-mortem privacy, which will assist in the transmission of digital assets on death, is vital. The position set out in this paper is, however, principled and the practical solution will be discussed more in the future work. The counterbalancing of such autonomy and property interests by countervailing interests is a further issue which will be dealt with in the author's future work.

Acknowledgments

The author would like to thank her PhD supervisor, Prof Lilian Edwards for her continuous support, invaluable insights and constructive criticism.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Horizon Digital Economy Hub, Nottingham; forms part of the work programme of the Research Councils UK funded Centre for Creativity, Regulation, Enterprise and Technology (CREATE); also supported by The University of Strathclyde King Hugh Fund; The Clark Foundation.

Notes

1. The definition of digital assets used herein is: 'widely and not exclusively to include a range of intangible information goods associated with the online or digital world, including: social network profiles (on platforms such as Facebook, Twitter, Google+ or LinkedIn); e-mails, tweets, databases, etc.; in-game virtual assets (e.g. items bought, found or built in worlds such as Second Life, World of Warcraft, Lineage.); digitised text, image, music or sound (e.g. video, film and e-book files); passwords to various accounts associated with the provision of digital goods and services, either as buyer, user or trader (e.g. to eBay, Amazon, Facebook, YouTube.); domain names; two- or three-dimensional personality-related images or icons (such as user icons on LiveJournal or avatars in Second Life); and the myriad of digital assets emerging as commodities capable of being assigned worth (e.g. 'zero day exploits' or bugs in software which antagonists can exploit).' See Edwards and Harbinja (2013b, 104–105).
2. Term 'code' is used here as introduced in Lessig's seminal work on the Internet regulation, meaning Internet architecture, technology, software, or in this case services aimed to enable an in-service control of post-mortem privacy and digital assets. See Lessig (2006).
3. See e.g. Fallon (1994, 876) 'Autonomy ... is a protean concept, which means different things to different people.'; or Rao (2000, 369) 'Autonomy itself is a complicated concept that incorporates multiple meanings.'
4. See Rappaport (2001, 443); Feinberg (1983, 483) asserts that the US Supreme Court 'in recent years appears to have discovered a basic constitutional right suggestive of our "sovereign personal right of self-determination," and has given it the highly misleading name of "the right to privacy"; Smith (1982, 175) states that autonomy is a 'pivotal constitutional value' in the US privacy cases and in other contexts; Henkin (1974, 1425); Nichol (1985, links privacy to ideal of self-governance.

5. As Atherton and Vines (1996, 34) observe: 'The ability of the testator to leave his or her property by will to whomever pleased him or her (the testator's testamentary freedom) was the dominant doctrine in the common law world for about 200 years before the twentieth century. The emphasis on the right to do what one liked with one's property reflected the succession theory of the time—the importance of the individual, the emphasis on free will, the importance of contract and the rise of capitalism'.
6. Locke regarded the power of bequest as part of paternal authority (1947, 156). Mill had utilitarian reservations about inherited wealth, but he maintained nevertheless that 'each person should have power to dispose by will of his or her whole property' (1878, 281). In his *Principles of the Civil Code*, Bentham thus asserted that: 'The power of making a will ... may ... be considered as an instrument of authority, confided to individuals, for the encouragement of virtue and the repression of vice in the bosom of families. ...' (1843, 337).
7. Naffine (2000) states that 'English law proceeds upon the basis that the deceased as a legal person does not survive his physical death'. Or Paton's *Jurisprudence* cited as authority for the proposition that 'most modern legal systems lay down the rule that, in cases where legal personality is granted to human beings, personality begins at birth and ends with death.' (Wood and Certoma 1990, 309). But also 'In the Anglo-American system of law, the dead have neither rights nor duties ... We may appoint a guardian ad litem to protect the expectant interests of the unborn. There is no guardian ad litem for the deceased because he has no interest.' (Simes 1955, 1).
8. The principle has been revised in the United Kingdom and now only pertains to causes of action for defamation and certain claims for bereavement. See generally Law Reform (Miscellaneous Provisions) Act 1934, c. 41, The 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.
9. In the Restatement (Second) of Torts, the American Legal Institute takes a stance similar to English law that a person's privacy interest ends upon his death. *Fasching v Kallinger* 510 A.2d 694, 701 (N.J. Super. Ct. App. Div. 1986) ('The general rule is: the right of privacy dies with the individual. The right of privacy is a personal right and cannot, as a general rule, be asserted by anyone other than the person whose privacy is invaded.');
10. 'the purely personal right of privacy dies with the person' *Miller v. Nat'l Broad. Co.*, 232 Cal. Rptr. 668, 680 (Ct. App. 1986); see also *Hendrickson v. Cal. Newspapers, Inc.*, 121 Cal. Rptr. 429, 431 (Ct. App. 1975) ('It is well settled that the right of privacy is purely a personal one; it cannot be asserted by anyone other than the person whose privacy has been invaded, that is, plaintiff must plead and prove that *his* privacy has been invaded. Further, the right does not survive but dies with the person.').
11. See Restatement (Second) of Torts § 652I (1977) ('Except for the appropriation of one's name or likeness, an action for invasion of privacy can be maintained only by a living individual whose privacy is invaded.').
12. For a survey of which states provide for the protection by common and statute law, see Edwards and Harbinja (2013a, 124); Also, for an interesting proposal of creating publicity rights in Scots law, which would extend on death but only if registered pre-mortem for the benefit of the beneficiaries according to the deceased's will, see Black (2009, 226–238).
13. *Jaggi v. Switzerland*, App. No. 58757/00, 47 Eur. H.R. Rep. 30 (2006); *Estate of Kresten Filtenborg Mortensen v. Denmark*, App. No. 1338/03, 2006-V Eur. Ct. H.R. (2006); *Koch v. Germany*, App. No. 497/09, Eur. Ct. H.R. (2012).
14. see Case C-101/01, *Criminal Proceedings Against Lindqvist*, 2003 E.C.R. I-12971, I-13027 (European Court of Justice decision deferring to the national court's resolution of the issue) ('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.').
15. 'Dead persons cannot give consent to use or changes in their personal data or contribute to any balancing of interests which may be required. Rights as data subjects should in general extend only to living individuals, but should be exercisable for a limited period after the

- death of the data subject by personal representatives.’ House of Lords Select Committee on the European Communities, *Report of the Protection of Personal Data* 1992.
15. Recital 27, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016.
 16. National Conference of Commissioners on Uniform State Laws, Drafting Committee on Fiduciary Access to Digital Assets, ‘Fiduciary Access to Digital Assets Act’, February 15–16, 2013, Section 4 of the Draft reads ‘Except as a testator otherwise provided by will or until a court otherwise orders, a personal representative, acting reasonably for the benefit of the interested persons, may exercise control over the decedent’s digital property to the extent permitted under applicable law and a terms-of-service agreement.’ This provision clearly favours terms of service agreements and lacks clarity for personal representatives.
 17. National Conference of Commissioners on Uniform State Laws, Drafting Committee on Fiduciary Access to Digital Assets, ‘Fiduciary Access to Digital Assets Act’, February 15–16, 2013, s. 8 (3) (b) ‘(b) any provision in a terms-of-service agreement that limits a fiduciary’s access to the 18 digital assets of the account holder under this [act] is void as against the strong public policy of 19 this state, unless the limitations of that provision are signed by the account holder separately 20 from the other provisions of the terms-of-service agreement.’

References

- Alexander, G. S., and E. M. Peñalver. 2012. *An Introduction to Property Theory*. Cambridge: Cambridge University Press.
- Allen, A. L. 1999. “Coercing Privacy.” *William & Mary Law Review* 40: 723–757.
- Atherton, R. 1988. “Expectation Without Right: Testamentary Freedom and the Position of Women in Nineteenth Century New South Wales.” *University of New South Wales Law Journal* 11: 133–157.
- Atherton, R. F., and P. Vines. 1996. *Australian Succession law: Commentary and Materials*. Sydney: Butterworths.
- Atwater, J. 2006. “Who Owns Email? Do You Have the Right to Decide the Disposition of Your Private Digital Life?” *Utah Law Review*, 2: 397–418.
- Baker v. Bolton. 1808. 1 Camp 493.
- Bennett, C. J., and C. D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: The MIT Press.
- Bentham, J. 1843. “Principles of the Civil Code.” In *The Works of Jeremy Bentham*, edited by John Bowring, 296–365. Edinburgh: William Tait.
- Bentham, J. 1948. *A Fragment on Government*, edited by Wilfrid Harrison. Oxford: Blackwell.
- Bernal, P. 2014. *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge: Cambridge University Press.
- Beverly-Smith, H. 2002. *The Commercial Appropriation of Personality*. Cambridge: Cambridge University Press.
- Beyer, G. W., and N. Cahn. 2013. “Digital Planning: The Future of Elder Law.” *NAELA Journal*, 9: 135–155.
- Black, G. 2009. “A Right of Publicity in Scots Law.” PhD diss., University of Edinburgh.
- Blackstone, W. 1829. *Commentaries on the Laws of England (1765–1769)*. Oxford: Clarendon Press.
- Cahn, N. 2011. “Postmortem Life On-Line.” *Probate and Property* 25: 36–39.
- Cohen, J. E. 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press.
- Cohen, L. E. 2000. “Examined Lives.” *Stanford Law Review* 52: 1373–1438.
- Conner, J. 2010–2011. “Digital Life After Death: The Issue of Planning for a Person’s Digital Assets after Death.” *Estate Planning & Community Property Law Journal* 3: 301–355.
- Darrow, J., and G. Ferrera. 2006. “Who Owns a Decedent’s E-Mails: Inheritable Probate Assets or Property of the Network?” *New York University Journal of Legislation and Public Policy* 10: 281–308.

- Desai, D. R. 2008. "Property, Persona, and Preservation." *Temple Law Review* 81: 67–122.
- De Waal, M. J. 2007. "A Comparative Overview." In *Exploring the law of Succession: Studies National, Historical and Comparative*, edited by K. Reid, M. J. De Waal and R. Zimmermann, 1–27. Edinburgh: Edinburgh University Press.
- du Toit, F. 2000. "The Limits Imposed Upon Freedom of Testation by the Boni Mores: Lessons from Common Law and Civil Law (Continental) Legal Systems." *Stellenbosch Law Review* 77: 358–384.
- Edwards, L., and E. Harbinja. 2013a. "Protecting Post-mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World." *Cardozo Arts & Entertainment Law Journal* 32 (1): 83–129.
- Edwards, L., and E. Harbinja. 2013b. "What Happens to My Facebook Profile When I Die?: Legal Issues Around Transmission of Digital Assets on Death." In *Digital Legacy and Interaction: Post-Mortem Issues*, edited by C. Marcel and V. Pereira, 115–144. Springer: Human-Computer Interaction Series.
- Etzioni, A. 2000. *The Limits of Privacy*. New York: Basic books.
- Fallon, H. R., Jr. 1994. "Two Senses of Autonomy." *Stanford Law Review* 46: 875–905.
- Feinberg, J. 1983. "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?" *Notre Dame Law Review* 58: 445–492.
- Friedman, L. M. 1966. "The Law of the Living, the Law of the Dead: Property, Succession and Society." *Wisconsin Law Review* 29: 340–378.
- Hackett, C., and U. Connolly. 2013. "Privacy from Birth to Death and Beyond: European and American Perspectives. Symposium Report." *SCRIPTed* 10: 123–128. <http://script-ed.org/?p=828>.
- Harbinja, E. 2013. "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could be the Potential Alternatives?" *SCRIPT-ed* 10 (1): 19–38.
- Harbinja, E. 2016. "Legal Nature of Emails: A Comparative Perspective." *Duke Law & Technology Review* 14: 227–255. <http://scholarship.law.duke.edu/dltr/vol14/iss1/10>.
- Hegel, G. W. F. 1967. *The Philosophy of Right*. Translated by Knox. Oxford: Oxford University Press.
- Henkin, L. 1974. "Privacy and Autonomy." *Columbia Law Review*. 74: 1410–1433.
- Hopkins, J. P. 2013. "Afterlife in the Cloud: Managing a Digital Estate." *Hastings Science and Technology Law Journal*. 5: 209–244.
- Kant, I. 1991. *The Metaphysics of Morals*. Translated by Mary Gregor. Cambridge: Cambridge University Press.
- Kant, I. 2003. *Observations on the Feeling of the Beautiful and the Sublime*. Translated by John T. Goldthwait tr. Berkeley: University of California Press.
- Kasket, E. 2013. "Access to the Digital Self in Life and Death: Privacy in the Context of Posthumously Persistent Facebook Profiles." *SCRIPTed* 10: 7–18.
- Lee, J. 2015. "Death and Live Feeds: Privacy Protection in Fiduciary Access to Digital Assets." *Colombia Business Law Review* 2: 654–704.
- Lessig, L. 2006. *Code, version 2.0*. New York: Basic Books.
- Locke, J. 1947. *Two Treatises of Government. Second Treatise*. Edited by T. Cook. New York: Hafner.
- Locke, J. 1979. *An Essay Concerning Human Understanding*. Edited by Peter Nidditch. Oxford: Oxford University Press.
- Mazzone, J. 2012. "Facebook's Afterlife." *The North Carolina Law Review*. 90: 1643–1685.
- McCallig, D. 2013. "Facebook after Death: An Evolving Policy in a Social Network." *International Journal of Law and Information Technology*, 1: 1–34.
- McCallig, D. 2014. "Data Protection and the Deceased in the EU." Paper presented at the CPDP, Brussels, January 24.
- Mill, J. S. 1878. *Principles of Political Economy*. London: Longmans, Green, Reader Dyer.
- Mill, J. S. 1984. *On Liberty*. Edited by Gertrude Himmelfarb. New York: Basic Books.
- Naffine, N. 2000. "When Does the Legal Person Die? Jeremy Bentham and the 'Auto-Icon'." *Australian Journal of Legal Philosophy*, 25: 79–95.
- Nichol, G. R. 1985. "Children of Distant Fathers: Sketching an Ethos of Constitutional Liberty." *Wisconsin Law Review*, 6: 1305–1357.
- Nissenbaum, H. F. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford Law Books.
- Ortiz, D. R. 1988. "Privacy, Autonomy, and Consent." *Harvard Journal of Law and Policy* 12: 91–97.

- Penner, J. 1997. *The Idea of Property in law*. Oxford: Oxford University Press.
- Perrone, M. 2012/2013. "What Happens When We Die: Estate Planning of Digital Assets." *Common Law Conspectus* 21: 185–210.
- Posner, R. A. 2008. "Privacy, Surveillance, and Law." *University of Chicago Law Review* 75: 245–260.
- Radin, M. J. 1982. "Property and Personhood." *Stanford Law Review* 34: 957–1015.
- Rao, R. 2000. "Property, Privacy, and the Human Body." *Boston University Law Review*. 80: 359–460.
- Rappaport, A. J. 2001. "Beyond Personhood and Autonomy: Moral Theory and the Premises of Privacy." *Utah Law Review* 2: 441–507.
- Rawls, J., and S. R. Freeman. 1999. *Collected Papers*. Cambridge: Harvard University Press.
- Raz, J. 1986. *The Morality of Freedom*. Oxford: Clarendon.
- Regan, P. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.
- Rosen, J. 2001. *The Unwanted Gaze The Destruction of Privacy in America*. New York: Vintage Books.
- Safranek, J. P., and C. J. Safranek. 1998. "Can the Right to Autonomy be Resuscitated after Glucksberg?" *Columbia Law Review*. 69: 737–757.
- Schneewind, J. B. 1998. *The Invention of Autonomy: A History of Modern Moral Philosophy*. Cambridge: Cambridge University Press.
- Schwartz, P. M. 1999. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review*. 52: 1609–1701.
- Sherry, H. 2013. "What Happens to Our Facebook Accounts When We Die?: Probate versus Policy and the Fate of Social-Media Assets Postmortem." *The Pepperdine Law Review*. 40 (1): 185–250.
- Simes, L. 1955. *Public Policy and the Dead Hand*. Ann Arbor: University of Michigan Law School.
- Smith, R. M. 1982. "The Constitution and Autonomy." *Texas Law Review* 60: 175–205.
- Solove, D. J. 2007. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 44: 744–772.
- Sonnekus, J. C. 2007. "Freedom of Testation and the Aging Testator." In *Exploring the law of Succession: Studies National, Historical and Comparative*, edited by K. Reid, M. J. De Waal, and R. Zimmermann, 78–99. Edinburgh: Edinburgh University Press.
- Tur, R. 1987. "The 'Person' in Law." In *Persons and Personality: A Contemporary Inquiry*, edited by A. Peacocke and G. Gillett, 116–129. Oxford: Basil Blackwell.
- Wood, O., and G. L. Certoma. 1990. *Hutley, Woodman and Wood Succession. Commentary and Materials*. Sydney: Law Book.