Death and Personal Data in the Age of Social Media

Egoyibo Lorrita Okoro
LLM Law and Technology
(2018-2019 Academic session)
ANR: 485937
SNR: 2019361

Thesis Supervisor: Dr. Bo Zhao
Second Reader: Ms. Hosna Sheikhattar
(December 2018)

Acknowledgement

To my family and friends whose support and encouragement made this thesis feasible, I say thank you.

To Dr. Bo Zhao for his patience and guidance, I say thank you.

Table of contents

Chapter 1 Introduction

> "The dead have no rights and can suffer no wrongs."
> - Sir James Stephen (1887)

1.1 Problem Statement

Privacy should survive death. Privacy should not have to erode at the expiration of human life, especially in an age where digitalisation is part of everyday life.[1] However, personal data protection is usually not accorded to the dead, nor are the dead considered *de facto* privacy rights bearers. Thus, leaving unprotected the surviving interests of the dead and those of their surviving relatives and/or heirs.

The current legal framework of the European Union does not have provisions for a posthumous data protection and/or privacy right – online and/or offline, nor is there a uniform law, globally, regarding the handling of deceased person's social media contents.[2] What this entails is that personal data of deceased persons are often left to the whims and caprices of Internet Service Providers (hereinafter referred to as ISPs) whom those with vested interests in the privacy and reputation of the deceased must challenge in order to preserve their interests; thereby incurring financial stress, dredging up painful memories and further inflicting emotional distress on the deceased's loved ones. All unnecessary burdens which can be mitigated or even effaced by the promulgation of posthumous personal data protection of deceased subjects as legal rights of the dead, or through other equally effective protective measures.

1.2 Background

It is axiomatic to state that we live in a Panopticon society in an epoch heavily preoccupied with human rights – social, economic and political, for all. With technological advancements come the digitisation of our everyday lives. Memories are created, collated, saved and shared in online spaces by us and by others, with or without our consent. Photos and videos, electronic communications and essays are increasingly made and saved on the cloud – Facebook, Dropbox, Google, Apple iCloud, etc., creating an uncountable amount of digitised assets with potential estate issues upon the maker's death. From train station to dance hall to college library, cameras are continuously awake and snapping and digital trails are studiously mapped, personal data collected and saved, even without the data subject's knowledge. Summarily, technology has turned our world into a sort of Panopticon where eyes are seemingly always upon us, even in the confines of our bedroom. Even Jeremy Bentham, the English social theorist and visionary designer of the Panopticon, could not have envisioned the plethora of surveillance cameras, mobile phones and other technological devices and networks that constantly watch and record

[1] Buitelaar,J. C. 2017. "Post-mortem privacy and informational self-determination", in: Ethics and Information Technology, Vol 19, pp.129-142.
[2] Zhao, S. B. 2016. "Posthumous Defamation and Posthumous Privacy Cases in the Digital Age", in: Savannah Law Review Vol. 3, No. 1

the personal data and/or activities of residents in public and, sometimes, private spaces in many – if not all – countries of the world. In the current socio-political climate of sousveillance – acts of video/audio/photographic recordings of events in a group by a participant – [3] and surveillance (the recordings of activities by political and corporate institutions with the aid of CCTV cameras, drones and other aerial surveillance systems), the Panopticon is no more a mere building, it has become a mechanism for social and political control, calling to mind Lawrence Lessig's assertion that there are four modalities of regulation: law, market, social norms and architecture (read: technology).[4]

As with every encounter of man with his society, these chronicling intrusions into man's privacy with the aid of new and emerging technologies in/and social networks have evoked questions of law, rights and obligations. Here, the question first posed by Lord Atkin in the *locus classicus* case of Donoghue v. Stevenson (1932), "who is my neighbour?",[5] becomes, for our globalising world, a socio-legal as well as socio-political question thrown at one and all, with the resulting answer echoing Lord Atkin's,[6] plus a mumbled: "everyone?". As modern technologies emerge, and social networks conform to these technologies, issues regarding posthumous personal data protection accrue, and with them, liability claims. In a visionary move, Facebook has updated their privacy and data protection policies to protect privacy following the death of account users. One of such policies is called the Legacy Contact which enables Facebook account users to mandate a trusted fellow Facebook account user to manage their account – without giving them undue access, for e.g., to messages – in the event of their death.[7] Twitter also has a likewise policy. However, these policies do not entirely protect the service user's personal data and privacy posthumously, as these policies are made by the corporations most often to suit their needs. And therein lies the issue: should the regulation of deceased persons' personal data and resulting privacy claims be left in the hands of private corporations?

Hence, the thesis aims to address what "digital privacy rights", if any, are available to residents within the European Union and cursorily in the United States of America, posthumously; and whether privacy rights of a dead person can be extended to include the wishes of surviving relatives, friends, testamentary beneficiaries, and the general public, for the sake of human dignity. The two jurisdictions were chosen for this research, not merely because of their substantial roles in the co-regulations of the globalised digital economy, but also because of their differing legal positions on privacy and data protection, especially with regards to posthumous considerations. These will be discussed further in chapter two.

---

[3] Mann, S. & Ferenbok, J. 2013. "New Media and the power politics of sousveillance in a surveillance-dominated world", in: Surveillance Futures, Vol. 11 No. 1/2.
[4] Lessig, L. 1999. Code and Other Laws of Cyberspace. Basic Books. New York, USA.
[5] Donoghue v. Stevenson [1932] UKHL 100.
[6] "The answer seems to be - persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question." – Lord Atkin, *id.*
[7] What is a legacy contact and what can they do? | Facebook Help Centre | Facebook Web. <https://www.facebook.com/help/1568013990080948 > Accessed: 16/03/2018.

1.3 Research questions

- New (and rapid) developments in Information and Communications Technology, over the last decade, have led to an increase in (posthumous) harms to both the dead and the living, do we need a posthumous data protection framework that directly protects deceased persons' personal data under EU law?
    - Why is posthumous data protection so important? What harm(s) can arise from a dearth of protection of deceased persons' data?
    - How do European Union Member States' laws – notably the laws of Germany and France protect posthumous personal data, online/offline?
    - What viable alternative approaches to ensuring posthumous data protection exist? Which of those alternative approaches is/are the best solution(s) for the European Union?

1.4 Aims and objectives

With this thesis the author hopes to contribute to existing literature in providing a better understanding of the "posthumous rights" in which digital afterlife and digital legacy increasingly matter to society. Julie Cohen in her article "What Privacy is for", opines that privacy has an image problem wherein it is seen as being "old-fashioned", "anti-progressive", "costly, and detrimental to organised society.[8] Privacy's image problem has resulted in a losing battle with national security and neo-liberal capitalism, whereby "digital privacy rights" are not taken seriously in cyberspace. This might explain the disregard – by law and man, for the "digital privacy rights" of those whom the law deems to be unworthy of its protection: the deceased.

"You are what Google says you are", opines Megan Angelo,[9] but what happens when Google says one thing and you are another? What happens when Google's "findings" are circulated and maintained upon your death, when you can no longer fight to protect your reputation? Addressing these issues, and more, while contributing to existing literature on Posthumous Privacy, is one of the aims of this thesis.

Hence, the research aims to propose and advocate a thinking beyond the "now" of privacy rights towards the "after-now" (inevitability of death) and the protection of privacy and personal data of deceased persons. Charles Sykes considers privacy to be a trait of human freedom,[10] and he is not wrong, for the European Union recognises people's rights to "inviolate personality", "right to reputation", and "right to privacy" – including the right to privacy in electronic communications.[11] But privacy and reputational harm after death remain beyond the scope of considerations for protection, only getting minimum consideration when a living person – with cause – is affected by

[8] Cohen, J. 2012. What Privacy is For. 126 Harvard Law Rev. 1904.
[9] Angelo, M. 2009. "You are what Google says you are". Wired, 12 Nov. 2009. Available at: < https://www.wired.com/2009/02/you-are-what-go/ > Accessed: 07/05/2018.
[10] Sykes, C. J. 1999. The End of Privacy. St. Martin's Press, New York.
[11] The European Convention on Human Rights (ECHR) at Article 8; *See* also Rotaru v. Romania [2000] ECHR 192

the actions of another with regards to a decedent's (digital) afterlife. Daniel Solove,[12] Daniel Sperling,[13] J. C. Buitelaar,[14] S. B. Zhao,[15] Floris Tomasini,[16] Jessica Hopper, and Edina Habinja and Lillian Edwards have researched and written on posthumous privacy and/or data protection.[17]

Lilian Edwards & Edina Habinja have written about the personal and economic interests in the digital world that can survive death,[18] from virtual gaming to e-commerce on ISPs' platforms to social media. Using case law from the US, UK, France and Germany as illustrations, they argue for a reconsideration of posthumous privacy along the lines of posthumous (inviolable) personality.

Stephen B. Zhao explored posthumous privacy and reputation and how they are regarded and protected generally. He distinguishes between posthumous privacy and reputation – where the former refers to the privacy issues that affect the dead, such as final resting places and protection of private personal information, the latter goes to the core of who the deceased was to and in society *ante mortem*. However, posthumous privacy and reputation are often tied to one another as the disclosure of private information can alter the ways society views a decedent.

Gianclaudio Malgieri postulated theoretical and practical solutions for the consideration, management and protection of posthumous personal data.[19] He argued for the legal protection of privacy *post mortem*, the commodification of personal data and the quasi-propertisation of personal data as possible solutions for the management of posthumous personal data, thereby obliterating or mitigating the exploitation and abuse of the personal data of deceased persons, and the harmful effects those may have on their surviving relatives.

However, the research done in this area of privacy and data protection – as they intersect with law and technology, are still very few. In writing this thesis, I hope to contribute my quota in advocating for a re-thinking of privacy as a "right" that transcends death.

---

[12] Solove, D. 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review; Solove, D. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review 745.
[13] Sperling, D. 2008. Posthumous Interests. Cambridge University Press, USA.
[14] Buitelaar, *supra* note 1.
[15] Zhao, *supra* note 2.
[16] Tomasini, F. 2017. Remembering and Disremembering the Dead – Posthumous Punishment, Harm and Redemption over Time. Palgrave Macmillan, UK.
[17] Edwards, L. & Harbinja, E. 2013. 'What Happens to My Facebook Profile When I Die?': Legal Issues Around Transmission of Digital Assets on Death. SSRN; *see also* Edwards, L. & Harbinja, E. 2013. Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. SSRN.
[18] Edwards & Harbinja. 2013. Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. SSRN.
[19] Malgieri, G. 2018. R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions. SSRN.

1.5 **Theoretical focus and limitation**

The research for the thesis was conducted from an interdisciplinary perspective, drawing upon fields such as legal theory, social theory and political theory. Therefore, the author studied regional and national statutory laws and case laws within the European Union and the United States of America, while drawing upon theories from social and political philosophy. To highlight how personal data is generally treated after death in Common law and Civil law jurisdictions, the author referred to certain U.S laws for illustrative comparison. However, the research for the thesis did not deploy a comparative analysis model, but merely relied on those U.S laws to underscore relevant points.

Moreover, as personal data is an exceptionally broad topic that permeates every aspect of our lives and every industrial activity that interlinks humanity to digitised life, this thesis focuses on those personal data that are inexorably linked to our digital (after)lives.

1.6 **Methodology and theoretical framework**

The research for the thesis was conducted using a qualitative approach which involved doctrinal, heuristic research, by reading, examining and analysing regional and national statutes and cases within the European Union, published and unpublished academic texts, and grey literature – newspaper and journal articles, literary publications, and organizations' reports and white papers.

McConville & Chui define qualitative research as that which has no dealings with numerals – non-numerical, as opposed to quantitative research which deals primarily with statistical data.[20] They also define doctrinal research as a research method that involves an inquiry into what a body of law says about a specific legal issue and applying that body of law to that legal issue.[21] Because it is a process that requires the explication of legal documents – the body of law, with the aim to apply the resultant findings to the relevant legal problems, doctrinal research was the ideal research method for the thesis, and proved to be crucial for the thesis research.[22]

To find research sources, the author first searched for texts with the following words/phrases in their titles: "privacy", "posthumous privacy", "post-mortem privacy", "privacy and reputation", "privacy and internet", "surveillance" and "research methods in law". These searches were conducted primarily through the author's Tilburg University Library Account which is powered by WorldCat Discovery (online). However, there are some other texts which the author discovered by scouring the Library's physical shelves and Google.com, and those others she discovered merely by following the trail of citations by those authors whose works she found informative and relevant to the research topic.

---

[20] McConville, M. & Chui, W. 2007. Research Methods for Law. Edinburg University Press, U.K.

[21] *Id*; *See also* Lomio, J., Spang-Hanssen, H., & Wilson, G. 2011. Legal Research Methods in a Modern World. Djof Forlag, Denmark.

[22] Hutchinson, T. 2017. "Doctrinal Research: Researching the Jury", in: Research Methods in Law, Watkins, D. & Burton, M. 2017 (eds.). Routledge, U.K.

1.7 Outline of the thesis

The thesis is divided into five chapters. Chapter 1 introduces the issue of privacy and reputation after death and explains the research methods and theories employed in researching the topic and analysing the research findings.

Chapter 2 deals with the issue of (posthumous) personal data protection, with a cursory look at the US common law system – in illustrative comparison to the EU's civil law system – and a deeper look at (posthumous) personal data protection under the (predominantly) civilian European Union. Where the former rejects any belief that personality rights survive the dead – with the exception of the right of publicity, the latter is generally accommodating of posthumous data protection but grapples with balancing posthumous interests with existing legal rights.[23] A good example of this dilemma is the privacy expectations of the deceased and their surviving relatives as opposed to the right to freedom of expression and information of the press (Articles 8 & 10 of the European Convention on Human Rights).

Chapter 3 discusses the legal stances of the European Commission and the legislative and judiciary organs of select EU Member States regarding posthumous personal data protection and the (possible) regulation of privacy and data protection in cyberspace.

Chapter 4 investigates what possible (alternative) approaches to protecting personal data posthumously might be feasible for EU Member States. Here, we look at: (1) self-regulation of Internet content as a solution for protecting personal data posthumously, in particular the measures being taken by Facebook, Google and Twitter; (2) the right of publicity provided under The US state of California, a Common Law jurisdiction that protects – under statute and case law, a person's right in his/her personal data. Under statute, the protected personal data is distinguished and categorised in five: name, voice, signature, photograph, and likeness (Section 3344 of the California Civil Code). Under case law, a four-step test is employed to determine if the right of publicity has been breached: use of identity, appropriation of name or likeness, lack of consent, and resulting injury.[24]

Chapter 5 wraps up all that had been discussed in the previous chapters, analyses findings according to research questions, and offers author's own recommendations for the regulation of posthumous personal data protection and digital privacy in our globalising world.

[23] Edwards & Harbinja (2013), *supra* note 17.

[24] *See* White vs. Samsung. 971 F.2d 1395 (9th Cir. 1992), *rehearing and rehearing en banc denied*, 989 F.2d 1512 (9th Cir. 1993), *cert. denied*, 508 U.S. 951 (1993).

Chapter 2 Legal Framework

> "You are what Google says you are."
>
> - Megan Angelo (2009)

This chapter examines the issue of (posthumous) personal data protection, under the US Common Law system, in opposition to the Civil Law system, however it takes a deeper look at (posthumous) personal data protection under the (predominantly) civilian European Union. Where the US legal system shuns any belief that personal rights survive the dead – with the exception of the right of publicity in some states, the latter is more sympathetic but battles with balancing those rights with other existing rights.[25] A notable example is the dilemma of: on the one hand, respecting the privacy of the dead – as it relates to the privacy of their surviving relations, and on the other hand, ensuring the living's right to freedom of expression and information (Articles 8 & 10 of the European Convention on Human Rights). Often the public interest in certain information clashes with an individual's right to privacy, as such courts have had to employ a balancing test to weigh which right trumps the other in any particular case.

2.1 What is personal data?

According to Article 4(1) of the General Data Protection Regulation (hereinafter: GDPR), personal data is any information or group of pieces of information that is/are connected to and can be used to identify and/or re-identify a living individual. If the information is irreversibly pseudonymised in such a way that it cannot be used to identify a living individual, it cannot be classified as personal data (Recital 26 of the GDPR). The key factor here is the *(re-)identification* of a living individual using the information in issue. According to the European Commission (n.d.),[26] the following are examples of personal data:

> "a name and surname; a home address; an email address such as name.surname@company.com; an identification card number; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; the advertising identifier of your phone; data held by a hospital or doctor, which could be a symbol that uniquely identifies a person".

It is pertinent to note that personal data when defined within the boundaries of medicine and death encompasses the definition provided under Article 4(1) of the GDPR plus biological/medical data for donation to institutions – blood, organ and tissues, gamete, stem cell, brain and limbs – for artistic, commercial, philanthropic and/or

[25] Edwards & Harbinja (2013) *supra* note 17.
[26] What is Personal Data? |European Commission (n.d.) |Web. < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en > Accessed 21/06/2018.

medical purposes.[27] Determining what biological/medical data fall under the definitive scope of personal data requires ascertaining whether the data is capable of identifying or re-identifying an individual. The human finger, for instance, does not qualify as an identifying element of personal data without the extraction of relevant information from it. The pattern on the finger, however, is a biometric data capable of identifying an individual.[28] According to Mark Taylor, the key to distinguishing between what human tissue qualifies as personal data is understanding the relationship between data and information.[29] Where data represents material for analysis, information is the outcome of that analysis.[30] Using blood samples as an example, he posits that blood is a source out of which biometric data is extracted, and not biometric data itself.[31]

2.2 Scope of personal data protection under the GDPR

The GDPR explicitly and repeatedly states that the protection of personal data is a right reserved for natural persons – with limitations in line with conformity with other rights (in Recital 4); and excludes (in Recital 27) the personal data protection of deceased persons, ensuring that recourse to posthumous protection or redress for harms will not be sought under the GDPR or at Union level. However, the GDPR does not prevent Member States from providing for posthumous personal data protection under their national laws, which means that states, if they so wish, can decide to protect posthumous under national laws.[32] This stance by the Commission is not surprising seeing as the commodification of personal data has turned online personal data into information goods synonymous with Big Data – a somewhat revolutionary business model that has become, in the words of Julie Cohen, "Wall Street's flavour of the month".[33] Gianclaudio Malgieri likens this stance to a copyright approach to privacy wherein "information multinationals" protect data subjects – treating personal data as *de facto* property – as "trade secrets".[34] Even as he acknowledges that defining access to and ownership of data is a tough challenge for any regime, he argues that the GDPR aspired to a "human right" approach to personal

---

[27] Krutzinna, J and Taddeo, M and Floridi, L. 2018. Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data. Available at SSRN: < https://ssrn.com/abstract=3177989 or http://dx.doi.org/10.2139/ssrn.3177989 > Accessed 30/09/2018.

[28] Taylor, M. 2012. Genetic Data and The Law: A Critical Perspective on Privacy Protection. Cambridge University Press, U.K. See also: Lunshof et al. 2008. "From Genetic Privacy to Open Privacy", in Science and Society, Vol. 9.

[29] *Id, at page 41.*

[30] *Ibid.*

[31] *Ibid.*

[32] The Lotus Principle in International Law follows the doctrine that where an act is not expressly prohibited by International Law, a sovereignty state is free to perform that act. For further reading, *see*: Hertogen, A. 2015. Letting Lotus Bloom. European Journal of International Law, Volume 26, Issue 4, Pages 901–926.

[33] Cohen, *supra* note 8.

[34] Malgieri, Gianclaudio, 'Ownership' of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution? (November 20, 2016). Journal of Internet Law, Vol. 20, n.5, November 2016. Available at SSRN: < https://ssrn.com/abstract=2916079 > Accessed 30/09/2018.

data protection but failed in providing a strong structure of property entitlement to data subjects.[35]

2.3 Scope of personal data protection in the United States of America

In the United States of America, there is no single, uniform legislation for the protection of personal data. Rather, protection is covered under federal and state legislations aimed at specific sectors with specific goals – consumer protection, electronic communications, and health information privacy, for e.g. Thus, the type of information protected depends on the provisions of each statute.[36] In protecting – at least, as protective as technological-innovations-loving US can be, privacy of residents, some states (for example, California, New York, and Massachusetts) are more proactive than others.[37] Specific coverage of US national and state legislations that aim to protect personal data ranges from consumer protection in the online and offline markets, as well as in the banking and health sectors, to restrictions to recording communications (the so-called two-party consent laws) to cyber security to child protection to publicity rights – right to one's own image.

Under US federal law, some notable legislations that aim to protect the personal data and thus privacy of individuals include:[38]

1. The Federal Trade Commission Act of 1914: this law prohibits unfair and/or deceptive practices by service providers online and/or offline, laying out privacy guidelines for companies providing services to consumers and sanctioning them where necessary, especially with regards to the unauthorised disclosure of personal data.
2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA): this law controls the collection, processing, handling, use and protection of medical information, thereby reducing healthcare fraud and abuse.
3. The HIPAA Omnibus Rule mandates entities to provide a notice to the relevant authorities when there has been a breach, or likelihood of a breach, of protected health information. This rule aims to strengthen the privacy and security protections for health information as established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
4. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) of 2003 regulates the collection and use of email addresses for commercial and non-commercial purposes. It aims to put an end to spamming.
5. The Telephone Consumer Protection Act of 1991 which amended the Communications Act of 1934, regulates the collection and use of telephone numbers for telemarketing.

---

[35] *Id* at pp. 7-8.
[36] Thoren-Peden, D.S & Meyer, C.D. 2018. Data Protection 2018: USA. Available at: < https://www.pillsburylaw.com/en/news-and-insights/data-protection-2018-usa.html > Accessed 30/09/2018
[37] *Ibid*.
[38] *Ibid*

6. The Electronic Communications Privacy Act of 1986 prohibits the interception of electronic communications – wiretapping and tracing, and unauthorised access to stored electronic communications.
7. The Computer Fraud and Abuse Act of 1984 prohibits computer tampering or any form of access to a computer without authorisation or outside the boundaries of authorisation.

Under US state laws, most notably the laws of California, there are statutes which aim to protect privacy of persons by prohibiting security breaches of stored personal information and requiring entities to provide notification of any breach to the relevant authorities. All 50 states of the US have enacted statutes to this regard.

In a progressive move, the US has come up with a law that provides fiduciaries – executors of wills and attorneys-in-fact, with a legal way of managing the digital assets of deceased or incapacitated people. The Revised Uniform Fiduciary Access to Digital Assets Acts (RUFADAA) was specifically enacted to protect digital assets and their management. Enacted in Georgia, Maine, Missouri, Virgin Islands, and West Virginia, RUFADAA protects the privacy of the deceased where they did not consent to the disclosure of their digital estate ante mortem. As such, an executor of an estate has no authority over the content of e-communications – private emails, chats, etc. However, where the deceased died intestate, the executor can gain access to other digital assets – audio-visual media, animations, photographs, word documents, etc., with the approval of the court. To gain approval, the executor must show proof why the disclosure is needed to properly administer the estate. Where a fiduciary does not have instructions by virtue of a will, trust or power of attorney, the custodian – the company who makes, stores, or provides the digital assets, can determine with the aid of its Terms of Service agreements with the deceased whether to comply with the Fiduciary's requests for access. Custodians may also request court orders, narrow down their compliance with requests by providing access to those assets that are "reasonably necessary" for the administration and conclusion of the deceased's estate, or refuse to comply with unduly onerous requests. For their compliance tasks, they may also charge fees. A custodian must not provide access to deleted assets or a jointly-owned account.

Another area where personal data and privacy are favourably protected under US state law is with regards to right to one's own image, name and likeness – the right of publicity. The right of publicity is the right of an individual – exercised by him/her or through his/her representative, to control the commercial use of his/her name, image, likeness, and/or any other form of identity.[39] Whereas, traditionally, under Common law, the right of publicity, like all privacy rights, dies with the deceased and descendants are estopped from bringing suits for recovery, now the right is being recognised as a posthumous right that can be enforced by the deceased's successors-in-title or estate administrator.[40] Currently, thirty US states now recognise publicity rights either through Common law – case law, or statute. Examples include California, New York, Kentucky,

[39] Smolensky, K.R. 2009. Rights of the Dead. Hofstra Law Review Vol. 37, 763; *see* also Park, S. and Sánchez Abril, P. 2016. Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights. *American Business Law Journal*,*53*(3), 537-598.
[40] Lugosi v. Universal Pictures, 603 P.2d 425 (Cal. 1979).

Washington, Texas, Minnesota, Ohio, Nevada, and Nebraska, to name a few.[41] Notwithstanding, the rights of the dead – where recognised, are time limited and erode with the passage of time;[42] this is also the case with the US states' recognition of posthumous publicity rights in the US. In Kentucky, publicity rights for public figures endure 50 years after the death of the right-holder, while in California, it is 70 years after the death of the right-holder.

Going by the Restatement (Third) of Unfair Competition, there are four elements which must be conjunctively present for a claim to right of publicity to prevail, they are: (1.) The defendant used the plaintiff's identity (2.) for the defendant's commercial (or other) advantage (3.) without the plaintiff's consent, (4.) causing injury. Of note, as shown by the court decision in Shaw Family Archives v. CMG Worldwide Inc. (2006), the laws on right of publicity cannot apply retrospectively to cover decedents who did not have that right at the time of their death.

However, US privacy and data protection framework is not as comprehensive as the EU's, nor is it as sympathetic to posthumous personal data protection as some European Union countries are. The reason for the former can be attributed to the US's reluctance to firmly regulate Information and Communications Technology (ICT), while the latter is because of the nature of US legal system which is based upon the Common Law. Under Common Law, the principle of *actio personalis moritur cum persona* prevail against posthumous data protection – i.e., personal causes of action die with the dead.[43] This is because it is generally believed that "the dead have no rights and can suffer no wrongs".[44] Therefore, defamation claims, breach of confidence claims, and wrongful dismissal claims even when instituted in the claimants' lifetime die with the claimants.[45] This Common Law position was illustrated in the case of Rose et al vs. Daily Mirror Inc. (1940), where the Court of Appeals of the State of New York held *inter alia* that there is no cause of action for a libellous material which impugns the memory of a deceased but does not reflect negatively on his surviving relatives.[46]

2.4 Why protect personal data and as such privacy (posthumously)?

The protection of privacy and human dignity is at the core of the concept of personal data protection, be it ante mortem or post mortem. To understand this line of thought, it is pertinent to explore mainstream theorisations of posthumous privacy. Posthumous privacy rights are often viewed and defined along three principal theories of rights – the Interest Theory, the Will/Choice Theory, and the Property Rights Theory.[47]

---

[41] Park & Sanchez-Abril (2016), *Supra* note 39.
[42] *Id.*
[43] Flynn v. Higham, 149 Cal.App.3d 677 (1983); Restatement (second) of torts, § 560 (1977): "One who publishes defamatory matter concerning a deceased person is not liable either to the estate of the person or to his descendants or relatives".
[44] Sir James Fitzjames Stephen, 1st Baronet
[45] Edwards & Harbinja (2013), *supra* note 16, at page 120
[46] Rose et al. v. Daily Mirror, Inc., 20 N. Y. S.(2d) 315 (App. Div. 2d Dept. 1940); *see* also Hughes vs. New England Newspaper Publishing Co. (1942).
[47] *Supra*, notes 12, 13, & 34; *see also* Malgieri, Gianclaudio. 2018. Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. Privacy in

Under the Interest Theory, rights are seen as having been established to protect, promote and benefit the interests of the right-holder, while Will theorists see rights as avenues to advance the right-holder's ability to manage his/her liberties with regards to the choice to relinquish or enforce others' duties owed to him/her.[48] One critical shortfall of the Choice Theory approach to posthumous rights is that rights which the right-holder did not anticipate and thus provide exercise of, cannot be accounted for;[49] this is especially the case with rights – moral and otherwise – that accrued at death. Whereas, under the Interest Theory, argues Kirsten Smolensky, the dead, although incapable of making real-time choices, are capable of being legal right-holders by virtue of surviving interests.[50] Smolensky further argues that it is best to analyse and adopt a regime for posthumous rights using the Interest Theory approach because under that prism, persons who are incapable of making choices – mentally incapacitated and infants – are recognised as (potential) right-holders.[51] The Property Rights theory looks at personal data as an economic resource, a property which must belong to someone. Thus, the crucial question, as asked by Nadezhda Purtova, is: whose property rights should personal data be?[52] When used to define, analyse or adopt posthumous personal data protection, the property rights approach make a strong case for the deceased, for example the US right of publicity.

Without posthumous personal data protection, the likelihood of harm to a decedent's surviving interests exists and increases. As Daniel Sperling rightly noted: "[…] even though a person may not survive her death, some of her interests do".[53] For example, the right of publicity (examined above) – which takes a property rights approach, survives up to 70 years, in some jurisdictions, after the death of the right-holder.

With the right of publicity in mind, it is clear that posthumous personal data protection is not only about the protection of privacy and reputation, but also about the protection of the economic interests of the deceased – i.e., his/her estate. Gianclaudio Malgieri tells us that "personal data is no longer a mere expression of personality but a strong economic element in the relationships between companies and consumers".[54] The information economy has witnessed exponential growth since former US Senator Al Gore allegedly promoted the development and backing of high speed connectivity, with Facebook, Google (including Google+, Youtube) and Twitter, to name a few, dominating as premier social media networks. Paul Levinson calls these social media platforms "new

---

Germany - PinG, n. 4, 2016, 133 ff. Available at SSRN: < https://ssrn.com/abstract=2916058 > Accessed 30/09/2018.

[48] Sperling, *supra* note 13, at pp. 52-53.

[49] *Supra*, notes 12 & 34.

[50] Smolensky, *supra* note 39.

[51] *Id.*

[52] Purtova, N. 2015. The Illusion of Personal Data as No One's Property. Journal of Law, Innovation & Technology. Vol. 7. Issue 1, Pp.83-111 at p. 83.

[53] Sperling, *supra* note 13.

[54] Malgieri, C. 2016. Property & (Intellectual) Ownership of Consumers' Information: A New Taxonomy of Personal Data. Available at SSRN: < https://ssrn.com/abstract=2916058 > Accessed 30/09/2018.

new media", different from "new media" forms like Yahoomail and traditional .com websites; this is due to their defining characteristic of being platforms that enable consumers to be the writers and producers of some of their own content.[55] A big lure of "new new media", he extrapolates, is the ability to provide platforms to the masses that are, on the surface, free of charge. However, these platforms are not free; they operate on a quid pro quo basis, wherein the account user submits his/her personal data and contracts to the commodification of his/her personal data for the benefit of the ISP. The problem with this business model is that it is not sufficiently, uniformly regulated to protect account users, most especially posthumously. Thereby, leaving impractical lacunas where there existed previously none.

It is not all gloom, though. The Internet is advantageous for humans; it has changed and eased the way we learn and conduct research and interact with others far and wide. The Internet's ability to broaden our worlds and our minds from the comfort of our rooms via access to a computer, tablet or mobile phone is one of its most endearing features. But the same dematerialised feature of the Internet that makes it possible for us to be "invisible", also makes it possible for us to be unwittingly and unkindly exposed.[56] The Internet has blurred the distinction between private and public spaces and growing at an exponential pace that is proving hard for existing laws to keep up with.[57] In this regard, the GDPR has tried to bridge that gap, but as explained in the previous section, posthumous personal data protection is not covered under the GDPR.

Personal data on cyberspace travels as fast and wide as it takes for the information to be inputted, thereby blurring the lines between information for public or private consumption. The problem with the free flow of personal data is that it is hard to track and/or control the data once it has been transmitted.[58] Take for instance, a post made on Facebook by a fictitious John Doe (resident in Netherlands) to a select group of "friends"; the same post can be shared – in this case, John is notified by Facebook, "copied and pasted", or "screen-munched" and circulated virtually, from Facebook to Twitter to Google+ to Instagram, leaving John completely open to various harms from defamation, to use of and judgement thereof of his personal data without his consent, to breach of privacy. Where John could follow up legally to restore his dignity and reputation, in the case of defamation of character in his lifetime, it becomes a huge issue when the personal data is exploited and abused upon his death. Under EU law and the national laws of the Netherlands, John's friends and/or family will have no recourse for the restoration of his good name. This is also applicable to privacy claims as well as reputational harm.

According to Zhao, the descendants of a deceased subject have two posthumous interests: privacy and reputation.[59] Those two interests are recognised under EU law distinctly. To address the latter, the definition of reputation supplied by Black's Law Dictionary will be applied: "a person's credit, honour, character, good name". Elizabeth

[55] Levinson, P. 2009. New New Media. Pearson, USA.
[56] Sykes, *supra* note 10.
[57] *Id.*
[58] Charles Sykes captured this candidly in his assertion that "[personal] data is like a prostitute; once it's on the streets, everybody has access to it." (*supra* note 10 at page 101).
[59] Zhao, *supra* note 2.

Anne Kirley goes further by asserting that we may have many reputations, each representing each society within we operate.[60] Kirley also affirms that there are two types of reputational harm that can arise because of our interactions online: (1) reputational harm arising from our or others' exposure through posts; and, (2) the disclosure of our personal data without our consent. Sometimes, these two types of reputational harm can collide and occur concurrently.[61] The protection of a deceased person's reputation is justified under three umbrella theories: in the interests of the deceased, in the interest of society, and in the interests of the deceased's relatives. It is in the interests of the deceased to not have false and defamatory information published about them. It is in also in the interest of public justice to not have such false and defamatory information in circulation, so as not to distort the truth. Moreover, it is in the interests of the deceased relatives not to have that information negatively impact the enjoyment of their own right to private and family life.

Under the ECHR, there is an open-ended provision for the right to privacy – including protection of reputation. According to the ECHR, everyone has a right to respect for his private and family life, home and correspondence, and states must not unjustifiably interfere with that right.[62] This mandate to states has, over the years, evolved to include: positive obligation to protect the right to privacy. In many cases the ECtHR has held that there exists a positive responsibility on the part of national governments to uphold the protection of residents' reputation and balance same with the right to freedom of expression. In Pfeiffer v. Austria, a journalist who had been accused of causing another person to commit suicide because of his harsh criticism linking the deceased to Nazism alleged that Austrian courts failed to protect his reputation and the ECtHR agreed with him. In K.U. v. Finland, the ECtHR held that Signatory States must proactively adopt measures to ensure respect for private life even in personal interactions between persons.

However, when it comes to posthumous privacy protection, which the court recognises,[63] the court is reluctant to fully accord protection to the dead. Rather, the court looks to protect the living whose personal lives and as such privacy are affected in one way or the other by that of the deceased. In Pannullo & Forte v. France, the court held that a delay in burial procedures was a violation of the private life of the parents of a deceased baby. In Znamenskaya v. Russia, the court held that the refusal by the Russian federation to establish the paternity of a woman's still-born child was a violation of her right to private and family life under Article 8 of the ECHR. In the Estate of Kresten v. Denmark, the court held that conducting DNA testing on a corpse did not constitute an interference with private life under Article 8 of the ECHR.

---

[60] Kirley, Elizabeth Anne. 2015. Reputational Privacy and the Internet: A Matter for Law? *PhD Dissertations*. 8. Available at: <https://digitalcommons.osgoode.yorku.ca/phd/8 > Accessed 30/09/2018.
[61] *Id* at p.3.
[62] Article 8(1) & (2), ECHR.
[63] In the Estate of Kresten v. Denmark, the ECtHR held that "it is settled law that an individual had rights under the Convention even after death".

Conversely, privacy, especially in cyberspace is hard to define, even harder is the articulation of harm from violations of privacy (van der Sloot 2016).[64] This is because the principle of *ratione personae* requires a claimant to establish that s/he has suffered, *a prior*, individually and to a degree from the violation of privacy (van der Sloot 2016). Where s/he cannot prove that, the suit will fall. To quote Bert van der Sloot (2016:418):

> "Article 8 ECHR, in the dominant interpretation of the ECtHR, only protects individual interests such as autonomy, dignity, and personal development. Cases that do not regard such matters are rejected by the Court".

Thus, John Doe making a claim for the circulation of his personal data online without his consent will grapple with establishing that he suffered from the privacy violation. Even if his matter were to be entertained by the ECtHR, if he dies while the matter is still under determination his relatives can only continue the matter if they too suffered from that violation, by virtue of Article 71 of the ECHR.

2.5 Conclusion

The courts are still battling with balancing the right to data protection with the right to freedom of expression. However, even as it is acknowledged that posthumous data protection is a growing ideal, it is imperative to note and insist that giant strides still need to be made to ensure full protection is accorded across boards. As it is now, the bulk of the responsibility for the protection of personal data, posthumously, lie with individuals (data subjects) who must take proactive steps, ante mortem, to ensure that their personal data and thus private life is not proclaimed from the rooftops, without their consent.

[64] Van der Sloot, B. 2016. "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities", in: Data Protection on the Move: current developments in ICT and privacy/data protection. Pp. 411-436. Springer, Dordrecht.

Chapter 3 Posthumous Data Protection under EU Member State Laws

"Eventually all things are known. And few matter."

- Gore Vidal

"The right of privacy is not merely a constitutional right; it also exists in the law of torts"

- Charles Sykes (1999)

3.1 Introduction

Chapters 1 & 2 above established the importance of and need for posthumous data protection because certain interests can and do survive death. Hence, this chapter will explore posthumous data protection within the European context; this will be done by addressing the research question proposed in Chapter 1: "how do European Union Member States' laws – notably the laws of Germany and France protect posthumous personal data, online/offline?

No European-wide legislation or case law provides for posthumous data protection, not under the Charter of the Fundamental Rights of the European Union or the European Convention on Human Rights, and not by the European Court of Justice nor the European Court of Human Rights.[65] As a matter of fact, (revised) recital 23 of the GDPR explicitly states: "the principles of data protection should not apply to deceased persons." Long before this provision, the ECtHR has held severally that Article 8 of the Convention on Human Rights which provides for a right to respect for one's "private and family life, his home and his correspondence" applies only to natural, living persons, and not to the dead, unless the deceased's privacy is tied to that of a living person whose suit lies before the court;[66] as such causes of action from the deceased to the living are non-transferable.[67]

---

[65] Harbinja, E. 2013. Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives? Scripted, a Journal of Law, Technology & Society. Web. < https://script-ed.org/article/eu-data-protection-regime-protect-post-mortem-privacy-potential-alternatives/ > Accessed: 16/03/2018.

[66] *See* Coudrec & Hatchette Filipacchi Associates v. France, where the ECtHR held that abuse of the decedent's likeness can cause mental distress and emotional pain to his descendants; Also, in Editions Plon v. France, the ECtHR indirectly protected the privacy and dignity of the deceased president by holding that the interim ban on the distribution of the book entitled *Le Grand Secret* ("The Big Secret") until the relevant courts arrive at a decision regarding the legalities of medical confidentiality and the rights of his descendants was necessary in a democratic society.

[67] Estate of Kresten Filtenborg Mortensen v. Denmark (2006); Volker und Markus Scheke GbR and Hartmut Eiffert v. Land Hessen (2010); Koch v. Germany (2012)

Also, it is pertinent to note that, "reputation" is not directly mentioned in Article 8 of the European Convention on Human Rights (ECHR) which provides for the right to respect for one's "private and family life, his home and his correspondence". However, in Article 10(2) the ECHR provides for the protection of reputation by referring to it as one of the legitimate reasons for the justification of an interference with the right to freedom of expression. The European Union Charter of Fundamental Rights (hereinafter "The Charter") provides in its Article 1 that "human dignity" is an inviolable that must be respected and protected.[68] A provision that closely mirrors Article 1 of the German Basic Law (*Grundgesetz*). In Article 7, the Charter provides for "respect for private and family life" (Article 7), but "reputation" is not mentioned explicitly in the text as a distinct right. Over the years, however, both courts have decided on cases

However, under national laws, Member States have been able to establish some forms of recognition of posthumous protection of personal data, most notably Iceland, Germany, France,[69] Italy,[70] Spain,[71] Estonia,[72] and Bulgaria. Iceland recognises a cause of action for posthumous defamation and penalises defaming the deceased. In Article 240 of the Icelandic Penal Code, it is established that defamation of a deceased person is subject to fines or an imprisonment for up to one year. Furthermore, if an act committed against a deceased person is punishable, the direct relatives of the deceased person are entitled to initiate civil litigation or request official prosecution.[73] In Bulgaria, the Personal Data Protection Act provides for posthumous data protection by enabling the heir(s) of the deceased data subject to exercise his/her rights to data protection.[74] In Italy, the heirs of a deceased person can bring an action on their behalf for the restoration of non-pecuniary damages.[75] Also, Article 9(3) of the Italian Data Protection Code provides that any entity with an interest in the deceased's personal data right – right to access, right to object, right to rectification and right to erasure, can apply to have those

---

[68] Charter of Fundamental Rights of The European Union (2000/C 364/01).

[69] DLA Piper, 2016. France adopts Law for a Digital Republic: key data provisions are a jump-start on the
GDPR. Available at: < https://www.dlapiper.com/en/us/insights/publications/2016/11/france-adopts-law-for-a-digital-republic/ > Accessed 30/09/2018.

[70] For further reading, *see*: Malgieri, G. 2018. R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions; Data Protection and Privacy: The Internet of Bodies, edited by Ronald Leenes, Rosamunde van Brackel, Serge Gutwirth & Paul De Hert (Brussels, Hart, 2018). Available at SSRN: < https://ssrn.com/abstract=3185249 > Accessed 30/09/2018.

[71] *Id.*

[72] *See* particularly § 12 Personal Data Protection Act (Estonia) which *inter alia* gives data subjects the freedom to decide what becomes of their personal data upon death. § 13 entitles select family members the right to decide on posthumous personal data processing of a decedent, for a period up to 30 years after the death of the data subject.

[73] Article 25(3), General Penal Code of Iceland. Available at:
<https://www.government.is/library/Files/General_Penal_Code_sept.-2015.pdf> Accessed 28/10/2018.

[74] Article 28(3), Personal Data Protection Act, Bulgaria.

[75] Italian Corte di Cassazione, SS.UU. n. 15350/2015; see also: Article 597(3), Italian Criminal Code.

exercised.[76] Malgieri (2018) likens this to a Kantian model that follows the principle of "Recht der Menschheit" which mandates that anyone can act to protect the *bona fama defuncti* of the deceased, thereby ensuring that a person's good reputation subsists even in death.[77]

For this thesis, however, we will look at the two Member States of the European Union with the highest protection for posthumous personal data: Germany and France.

3.2 Posthumous data protection in Germany

German case law on the right of personality grew from provisions laid down in several statutes: the Basic Law (*Grundgesetz*), the German Penal Code (*StGB*),[78] the German Civil Code (*BGB*),[79] and the Act on Copyright and Related Rights (*Urheberrechtsgesetz, UrhG*).[80] Personal data is protected posthumously in Germany via reliance on the provisions of the 1949 constitution of the Federal Republic of Germany – Basic Law (*Grundgesetz*), which lays down the fundamental structure and essential values of the State.[81]

Article 1 of the Basic Law provides that human dignity shall be inviolable and mandates the state to respect and promote it.[82] The Act on Copyright and Related Rights (*UrhG*) provides for the moral rights of authors – based on the French concept of *droit d' auteur*,[83] including the right to determine how and when his/her work shall be published, the right to be identified as the author of his/her work, and the right to prohibit the distortion of his/her work or any other derogatory treatment of such which might affect his/her interests in the work.[84] Following a monistic conception of rights, these moral rights subsist as long as economic interests in them prevail.[85] The German Civil Code (*BGB*) provides for the right to one's own name; the law also provides that 'a person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable for compensation to the other party

---

[76] Codice in materia di protezione dei dati personali, d.lgs. 196/2003.
[77] Malgieria (2018), supra note 19, at page 14.
[78] German Penal Code (*StGB*). Translation provided by Prof. Dr. Michael Bohlander. Available at: < https://www.gesetze-im-internet.de/englisch_stgb/index.html > Accessed 01/10/2018.
[79] German Civil Code (*BGB*). Translation provided by the Langenscheidt Translation Service. Available at: < https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p3489 > Accessed 01/10/2018.
[80] The Act on Copyright and Related (*Urheberrechtsgesetz*). Translation provided by Ute Reusch. Available at: < https://www.gesetze-im-internet.de/englisch_urhg/index.html > Accessed 01/10/2018.
[81] The Basic Law (*Grundgesetz*). Translated by: Professor Christian Tomuschat and Professor David P. Currie. Available at: < https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0026 > Accessed 01/10/2018.
[82] *Id.*
[83] World Intellectual Property Organisation (WIPO). 2016. Understanding Copyright and Related Rights. Available at: < http://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf > Accessed 01/10/2018.
[84] *Urheberrechtsgesetz, UrhG, supra* note 80, at Ss. 12, 13, & 14.
[85] Edwards & Harbinja (2013), *supra* note 17, at page 130.

for the damage arising from this'.[86] In another statute – the German Penal Code (*StGB*), it is criminal to violate the intimate privacy of another by taking and sharing unauthorised photographs; it is also punishable by fine or imprisonment for up to two years to disparage the memory of deceased persons.[87] Following on these provisions, German courts have ruled over the years that the right to human dignity does not die with a deceased, even in circumstances where the right to human dignity clashes with the right to artistic freedom and expression.[88] So, even though there is no explicit statutory provisions to that effect, the case law of the Federal Constitutional Court of Germany (*BVerfG)* provides protection for the right of personality – including the right of publicity and the right to have one's personal information published only with his/her consent; Thereby ensuring the posthumous protection not only of human dignity – and therefore reputation, but also of privacy.

The right to have one's personal information published only with his/her consent fall under Robert Post's Three Concepts of Privacy, where he posits that privacy is connected to the creation of (public) knowledge, to the need not to have misleading information published about oneself such that the public hold the misleading information to be the truth.[89] Following a Millian ideology of freedom,[90] Post's postulations bear credence to the principle that the only justification for the curtailment of one's rights – especially the right to freedom of expression, is for the protection of another where the former's actions (might/will) directly violate those of the latter.

In the Lüth case,[91] the Federal Constitutional Court of Germany (*BverfGE)* affirmed the importance of upholding the basic right to freedom of expression in a free and democratic society but drew attention to the inherent effect(s) of the opinion on others, and the need to protect those as well. The court concluded that the basic right in Art. 5 of the *Grundgesetz* protects not only the utterance of an opinion as such, but also the effect it has on others; the court determined that in such situations a "balance of interests" is called for. The implication of this decision for posthumous personal data protection being that where A opines that B – a deceased entrepreneur, for e.g., was a religious bigot and this utterance causes the deceased's company's stocks to fall, the interests of the maker of the opinion must bow to the former interest.

In BvR 240/04, the Federal Constitutional Court of Germany (*BverfGE*) held that "the general right of personality ensures that an individual can himself determine how he presents himself to the public",[92] as such an artistic manipulation of the claimant's face to

---

[86] The German Civil Code, *supra* note 79, at Ss. 12 & 823(1).
[87] The German Penal Code, *supra* note 78, at Ss. 201a & 189.
[88] *Supra* notes 1, 34 & 54
[89] Post, R. 2001. Three Concepts of Privacy. Faculty Scholarship Series, Vol. 185.
[90] Mill, J.S. 1859. On Liberty. Available at: <https://eet.pixel-online.org/files/etranslation/original/Mill,%20On%20Liberty.pdf> Accessed 28/10/2018.
[91] 1 BvR 400/51; translation supplied by: Tony Weir, University of Texas at Austin. Available at: <https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=1369> Accessed 30/09/2018.
[92] BvR 240/04. Translation provided by Raymond Youngs, University of Texas at Austin. Available at: < https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=1499 > Accessed 30/09/2018.

distort his real image while making it seem original without his consent is a violation of his right to inviolable personality.[93] This line of reasoning follows from that in the Lüth case, and draws attention once again to the Millian harm principle which allows for limitations of liberty for the protection of the rights of others.[94] John Stuart Mills' position ties in neatly with the German dignitarian position and makes for a strong argument in support of posthumous data protection, at least in civil law jurisdictions that generally open to acknowledging that certain rights and causes of action survive death.

In the Mephisto case,[95] a Nazi era novel written by Klaus Mann portrayed Gustaf Grundgens as a character in the novel and in unfavourable lights. Even though the author denied any likeness of the character to a real person, the Federal Constitutional Court of Germany (*BVerfG)* held that the human dignity of the deceased covered under Article 1 of the Basic Law was of overriding importance and surpassed the constitutional right to artistic freedom under Article 5. The court also ruled that:

> "only a living person is […] entitled [to] the right of personality […]. An essential precondition of the basic right [to personality] is the existence of at least a potential or a future person. It is irrelevant that a person may be affected during his lifetime by what the legal situation will be after his death […]. It is no derogation from the freedom of action and self-determination guaranteed by [the basic right to personality] to hold that the protection of the personality expires on death".

It can be deduced from this that under the German Legal System, "death does not terminate the duty of the state to protect individuals from assaults on dignity".[96] But, the right of personality is one accorded to the living – heirs for instance, and not the dead.

In the Marlene Dietrich case,[97] the German Supreme Court (*BGH*) ruled that a right to damages for unauthorised commercial use of personality exists even when the person whose image/likeness was used had passed away. Thus, such a right pass to his/her heir, to be exercised in accordance with the explicit or presumed will of the deceased. This stance can be likened to the U.S right of publicity, in that the court recognises that there is a property interest in personal data that can survive death.[98]

The strongest case against posthumous privacy is that it has the potential to hamper the rights to freedom of expression and information – matters of public interest, resulting in incomplete archival and historical records.[99] However, "the freedom of

---

[93] *Id.*
[94] "That the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others." – John Stuart Mill (1859), *supra* note 90 at page 13.
[95] BVerfGE 30, 173.
[96] Rosler, H. 2008. Dignitarian Posthumous Personality Rights – An Analysis of U.S. & Germany Constitutional and Tort Law. Berkeley Journal of International Law. Vol. 26. No. 153
[97] BGH 1 ZR 49/97; translation provided by Raymond Youngs, University of Texas at Austin. Available at: < https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=726 > Accessed 30/09/2018.
[98]Smolensky, *supra* note 39.
[99] Edwards & Harbinja (2013), *supra* note 17, at p. 142.

expression of one individual stops at the door of privacy of another".[100] As can be seen by the decisions in the two cases cited above, the German courts are reluctant to override the right to human dignity even in the face of the right to freedom of expression – both of which are covered in the Basic Law. To determine who has a better claim when two constitutional rights are involved, the courts often weigh the two competing values against each other.[101]

In the Strauß Caricature case, the German court held that a caricature of Bavarian Prime Minister Straub which portrayed him as a pig is an attack on personal honour as protected under Article 1(1) of the Basic Law, and there can be no reliance on freedom of artistic expression (Article 5(3)) for such caricature.[102] In that case, the Prime Minister had sought prosecution for defamation before a lower court and succeeded, on appeal to the regional court, the verdict was vacated and the complainant acquitted. On further appeal on points of law to the regional court of appeal, the court upheld the finding of the court of first instance and found the complainant guilty for defamation on three counts. In the court's reasoning, the artist intentionally on all three aimed to dishonour the Prime Minister by comparing him and the Civil Party to copulating pigs. The very act of likening and/or comparing someone to a copulating pig was borne out of contempt and was therefore defamatory.

In the Caroline von Monaco case, the German Constitutional Court ruled that because the princess was a public figure, there was no breach of privacy by journalists who trailed her and her children for photographs, thus allowing for the artistic freedom of the photographing journalists.[103] It is worthy to note that the ECtHR found that the German courts had not failed in their duty to comply with obligations and no violation of Article 8 of the ECHR arose thereof.[104]

In BGH III ZR 183/17, the Federal Court of Justice of Germany held that access to a deceased's Facebook account cannot be granted to the parents under inheritance law because it will be an intrusion into the private communications between the deceased and others on the social networking site.[105] In that case, the parents of a deceased teenager had sought to gain to her Facebook account which she opened with their consent at the age of 14. However, upon keying in the relevant security access codes – username and password, they could not gain access to the account because Facebook had had the account memorialised upon the notification by a third party of the death of the account user. The parents brought a suit before a district court to compel Facebook to grant them access to the account as they were the heirs and legal representatives of the deceased.

---

[100] Kozyris, P. J. 2007. Regulating Internet Abuses: Invasion of Privacy. Kluwer Law International. The Netherlands, at p. 3.
[101] Smolensky, *supra* note 39, at p. 164; *See also*: Caroline von Monaco II & III BGH & BGHZ.
[102] BVerfGE 75, 369 1 BvR 313/85. Translation provided by Nomos Verlagsgesellschaft. Available at: https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=634. Accessed 01/10/2018.
[103] Caroline von Monaco III. Available at: < https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22699729%22],%22itemid%22:[%22001-61853%22]} > Accessed 28/10/2018.
[104] *Id.*
[105] Available at: <https://openjur.de/u/2110135.html> Accessed 28/10/2018.

They needed access to the account to discount the civil claims by the subway driver that the deceased had committed suicide. The district court applying the law on inheritance, ordered that access be granted to the plaintiffs on the ground that Facebook posts are akin to journals and diaries and as such can be inherited by the deceased's successors-in-interests under the community of heirs. On appeal to the Federal Court of Justice of Germany, the appellant court likened the communications on Facebook to that of telecommunications and ruled that such communications must be protected for the sake of those others other than the deceased, irrespective of their (assumed) testamentary wishes.

The above case is an interesting one because it comes at a time when the determination of one's digital afterlife is a hot topic in academia and in the media, with many demanding for co-regulation measures by/from the technology industry and governments. As of 2012, there were an estimated 30 million deceased Facebook users.[106] This has psychological effects on how we mourn on cyberspace. Astrid Hovde (2016) citing the memorialisation of the Facebook account of a deceased classmate felt that the activities on the page were as if the deceased were still alive, albeit digitally.[107] However, she also noted that the memorial page felt safe and comforting.[108] Cesare & Brandstad (2017) made observations along same lines, noting that for many people following a Facebook memorial page it feels like sitting in the living room of the deceased with his/her family and reminiscing.[109] The attitude is slightly different on Twitter where people passionately mourn celebrities they never met in real life. Interestingly, Michael Jackson is still tweeting on Twitter – an account he opened and operated before his death in 2009, commanding a followership of 1.94 million people.[110]

3.3 Posthumous personal data protection in France

In France, there are three sources of law from which national laws and binding rules originate:[111] (1.) The constitution – currently of the Fifth Republic; (2.) International Treaties;[112] and (3.) Legislation. Based on the structure of the Napoleonic Code, *Civil des Francais,* adopted in March 1804, statutes are supreme, court decisions do not set

---

[106] BBC, 2016. Facebook is a Growing and Unstoppable Digital Graveyard. <http://www.bbc.com/future/story/20160313-the-unstoppable-rise-of-the-facebook-dead> Accessed 28/10/2018.
[107] Hovde, A.L.L. 2016. Grief 2.0: Grieving in an Online World. Available at: <https://www.duo.uio.no/bitstream/handle/10852/52544/Hovde-Master-2016.pdf?sequence=5> Accessed 28/10/2018.
[108] *Id.*
[109] Cesare, N. & Brandstad, J. 2017. Mourning and Memory in The Twittersphere. Journal Mortality: Promoting the Interdisciplinary Study of Death and Dying. Volume 23 Issue 1, Pp. 82-97.
[110] Splinter. These are The Most Influential Dead People on Twitter. Available at: <https://splinternews.com/these-are-the-most-influential-dead-people-on-twitter-1793855156 > Accessed 28/10/2018.
[111] Newman, S. 2011. The Development of Copyright & Moral Rights in the European Legal System.
[112] *Id*; France follows the monist theory of International Law wherein treaties become part of national law when signed and take precedence over national legislation.

precedents and cannot make ensuing rules for France.[113] This defeats the principle of *stare decisis* such that French courts are not bound to take the prior decisions of another court into account when deciding a case before them and no court decision may take precedence over that of another. This is, in theory, the applicable system; in practice, decisions of superior French courts carry more weight for lower courts.[114] Notwithstanding, French courts have over the years ruled decisively on posthumous privacy and personal data protection claims.

French law distinguishes between economic and personal facets of personality rights, a dualistic conception of rights which means that for authors and creators of artistic works, moral rights are perpetual.[115] This also means that personal causes of action are non-transferable.[116] In SA Editions Plon v. Mitterand,[117] the Court of Cassation (*Cour de cassation*) – France's court of last resort – held that the right to act in respect of a privacy invasion ceases to exist when the sole holder of that right dies. In that case, the plaintiffs were M. and Me Mitterand, the deceased former President of France. They claimed that the book *Le Grand Secret*, which was a biography of Mr. Mitterand published by SA Editions Plon, disclosed personal information about him without authorization, especially with regards to the health of the President. They claimed a violation of the right to privacy and a breach of medical confidentiality. The Court of Cassation dismissed the claim based on the alleged invasion of the privacy of M. Francois. Mitterand because the private information published in the book formed only a small part of it and the information did not negatively affect the interests of the surviving relatives, but held the author and the publisher, SA Editions Plon, liable in damages for breach of medical confidentiality. Here, the court made recourse to the provision of Article 4(2) of the Code of Medical Ethics which provides for medical secrecy between a doctor and his/her patient during treatment. The court on this ground upheld the injunction against the further distribution of the book. In the court's reasoning, even if some violations of privacy occurred in the book and could have given rise to civil liability under article 9 of the Code Civil, the violations constituted a small portion of the book itself and thus would not necessitate a prohibition of distribution. However, the breach of medical confidentiality which featured in the book were covered by the Code of Medical Ethics which demands medical secrecy in favour of the patient; as such, the applicants were entitled to damages.

Posthumous personal data is protected in France under the Digital Republic Act – *Loi n°2016-1321 pour une République numérique*,[118] a fully GDPR-compliant legislation

[113] *Id.*
[114] *Id*, at page 10.
[115] *droit d'auteur; supra* notes 17 & 65.
[116] *Id.*
[117] JCP 1977. II. 22894. Translation provided by Tony Wier. Available at: <https://law.utexas.edu/transnational/foreign-law-translations/french/case.php?id=1240> Accessed 01/10/2018.
[118] *Loi n°2016-1321 pour une République numérique.* Available at: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id > Accessed 3/11/2018.

that came into force before the GDPR.[119] The law amends other laws regulating diverse aspects of the French digital economy and introduces new provisions for the regulation of that digital economy. The Digital Republic Act mandates internet service providers to inform users of what becomes of their personal data upon death.[120] The ISPs must allow service users to decide whether their personal data should be transferred when they die. The law devises an unprecedented new way and rights for individuals to decide how their personal data may be processed after their death. Prior to death, any person may give general or specific instructions – or both – regarding the storage, deletion or disclosure of his/her personal data, and/or the inheritance of his digital assets.[121] The instructions may be edited or revoked at any time – during his/her lifetime, by the data subject.[122]

Under the Digital Republic Act, general instructions concern and apply to all data that are collected and processed about an individual. These instructions may be registered with and kept by a certified third party or the National Commission on Informatics and Liberty (CNIL). The CNIL is responsible for managing a single entry for all general instructions and where they are kept. An individual may also send specific directives to a given data controller detailing how it may continue to use the personal data it holds about the data subject after his/her death. The controller upon receipt of the specific directives must comply with the wishes expressed therein when processing that individual's personal data after his/her death. This right cannot be waived in/by the controller's general terms and conditions of use. This is especially interesting considering the restrictive language in the terms of service of online platforms such as Twitter, Facebook, and Google+, which we will discuss in the next chapter. The Digital Republic Act poses a huge problem for those social networking sites, such as Facebook, who refuse to cede digital assets to heirs whilst relying on the protection of contract law. Facebook cannot rely on its Terms of Service as a defence, so barring that, it would have to comply with requests for disclosure of a deceased user's digital assets to his/her heirs. But, if Facebook decides to fight the law and deny the request, it would most likely rely on the GDPR and argue for the protection of the privacy and data protection of the living whose communications with the deceased would leave them open to invasion.

The data subject may also designate someone to execute the instructions and ensure they are complied with.[123] Where no such person is designated by the decedent and no instructions to the contrary, his descendants may execute the instructions themselves. Thus, "the problem of the subject" – *action personalis moritur cum persona* – which plagues posthumous data protection is resolved through the drafts of advance instructions by the data subject.[124] In the absence of any instructions by the data subject

---

[119] Malgieri, *supra* note 19, at page 15.
[120] *Supra* note 118, at Article 63.
[121] *Id*, at Article 63.
[122] *Ibid*. *See also*: DLA Piper, *supra* note 55; FieldFisher. 2016. France Adopts Digital Republic Law. Available at: <https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law> Accessed 01/10/2018; Dreyfus. 2017. Part 3: French Digital Republic Law – right to privacy. Available at: <http://www.dreyfus.fr/en/new-technologies/part-3-french-digital-republic-law-right-to-privacy/> Accessed 01/10/2018.
[123] *Supra* note 118, at Article 63.
[124] Malgieri, *supra* note 19, at p. 16.

upon his/her death, the legal successors of the decedent may exercise the posthumous data protection rights of the deceased.[125]

The Digital Republic Act also made away with France's previous legal requirement on data residency which mandated that all data be stored within the EU and not be transferred outside the Union. As such, businesses with a base in France can transfer data outside the EU if they abide by GDPR provisions on transborder data transfers. In this way, the thorny issue of multiple processors of personal data is left in the oeuvre of the scope of the GDPR. However, issues regarding enforcement where there are multiple processors, within and outside the EU, of posthumous personal data are left vague. Hopefully, future suits before the courts in the coming years will address those issues.

3.4 Conclusion

Posthumous reputation arises from an aggregation of the acts and traits performed and exhibited by a decedent while he/she was alive; whereas posthumous privacy refers to such matters as the choice of and/or respect for a resting place, non-disclosure of personal information.[126] Two distinctive interests that run on two divergent yet interconnected lines: "to be let alone" and "to rest in peace".[127] As can be seen from the above section, the Germany legal system follows a Kantian model wherein human dignity and personal data protection transcend death. Ensconced in the Civil Code, a right to protect one's personal data – name, image, from derogation, the provision on the right to one's name echoes Immanuel Kant's position that a good name is a congenital possession that survives death – *bona fama defuncti*.[128] According to Kant, to spread charges against someone who is by the very nature of death incapable of defending himself is mean-spirited.[129] Thus, it is not surprising that German courts are reluctant to waive aside such charges, even for the sake of the right to freedom of expression.[130]

Edwards & Harbinja tell us that there are two types of post-mortem privacy claims that can arise: (1.) a negative post-mortem privacy to keep matters secret after death – a classic Warren & Brandeis "right to be let alone";[131] and (2.) a positive post-mortem privacy claim for the right to control one's image or brand after death.[132] The German and French case laws and statutes illustrate these. Where *Mephisto* falls under the negative post-mortem privacy claim to be let alone, the *Marlene Dietrich* case falls under the latter; The French Digital Republic Act supports both claims. By providing data subjects with an informational self-determination – including the right to posthumous data protection, the French Digital Republic Act succeeds in narrowing the gap in the rapid progression from collection to processing to dissemination of personal information

[125] *Supra*, note 118, at Article 63.
[126] Zhao, *supra* note 2, at pp. 3-4.
[127] *Id*, at p. 4.
[128] Immanuel Kant. 2017. The Ethics of Immanuel Kant: Metaphysics of Morals – Philosophy of Law & the Doctrine of Virtue. Musaicum Books.
[129] *Id*.
[130] The *Mephisto* case.
[131] Warren & Brandeis. 1890. The Right to Privacy. Harvard Law Review. Vol. IV, No. 5.
[132] Edwards & Harbinja (2013), *supra* note 17, at p. 147.

which cumulatively ensure that control of those personal information is not in the hands of the data subject.[133]

Furthermore, Robert Post's Three Concepts of Privacy sums up this duo perfectly. Where the German stance on (posthumous) personal data protection follows a more traditional, classic model of human dignity that abhors distortion of one's image in the public's eye; France's recent legal developments in the field of (posthumous) personal data protection is more modern and anticipates the effects of digital technological changes on individuals' freedoms and the enjoyment of their right to privacy and data protection.

However, these legal developments – although, welcome and transformative for our current time, are not enough to protect posthumous personal data in this rapidly evolving digital age. For one, new technologies will arise faster than laws will be amended or made, that is assuming that more EU Member States are open to protecting personal data posthumously. Secondly, law works *ex post* and takes time and resources to enforce, as such law is not always the easiest option for ensuring the protection of personal data posthumously. Thirdly, not everyone will try to enforce their rights or those of their deceased loved ones by initiating proceedings before a judge, that is assuming the relevant jurisdiction recognises and protects those rights. Fourthly, the dematerialised, yet global nature of cyberspace makes it cumbersome for data subjects or their family/personal representatives to enforce rights to data protection, where one controller is based in another jurisdiction and the data subject in another. Thus, the need for more modern, radical approaches to posthumous data protection in cyberspace and in the physical world. We will address these alternative approaches in chapter 4 below.

[133] Solove (2006), *supra* note 12, at p. 488.

Chapter 4 Alternative Approaches to Posthumous Personal Data Protection

> **"**The governance of cyberspace is no less a pluralistic endeavour than is the governance of physical territory".
>
> - Chang & Grabosky (2017)

4.1 Introduction

As can be seen from chapters 2 & 3 above, the posthumous protection of personal data is not taken seriously in some jurisdictions – US and EU. This leaves one with further doubts: "what viable alternative approaches ensuring posthumous data protection exist?"; which of those alternatives is/are the best solutions for the European Union?" Three approaches come to mind and they will be addressed critically by examining the factors that influence or regulate behaviour, online and offline. According to Harvard Law Professor, Lawrence Lessig in his now critically acclaimed essay presented at Taiwan Net '98 conference in Taipei "The Laws of Cyberspace", there are four constraints that regulate behaviour in cyberspace. The behaviour and treatment of the personal data of others by platform users and also included – screenshots, downloads, access to posts, chats, comments, etc. For Lessig, these constraints are: law, social norms, the market, and architecture.[134]

With the above-mentioned questions as guides, this chapter will examine the following three alternative approaches to posthumous data protection through the lens of Lawrence Lessig's pathetic dot theory:[135]

1. Quasi-propertisation of personal data. The right of publicity provided under many US states is a good example of this quasi-propertisation model. The US state of California, a Common Law jurisdiction protects – under statute and case law, a person's right in his/her personal data. This is discussed in sections 4.3 and 4.4 (below).
2. Self-regulation of internet content as a solution for protecting personal data posthumously, the measures being taken by Facebook, Google and Twitter. This is discussed in section 4.2 (below).
3. Posthumous medical data donation through advance health directives/instructions, discussed in section 4.5 (below).

---

[134] Lessig, L. 1998. The Laws of Cyberspace. Available at: <https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf> Accessed 05/10/2018

[135] *Id.*

4.2 Law as a regulator of behaviour in cyberspace

The elements of liability which apply offline also apply online, even though the chances of just rewards are lower than in the offline world. This is due to the dematerialised, global nature of the internet wherein identifying the party in breach becomes an issue that transcends jurisdictions, calls for special technological expertise and the cooperation of ISPs.

The GDPR is a good example of a wide-reaching legislation that controls how others – usually businesses, treat personal data of others in cyberspace. However, as was established in chapters 2 and 3, the GDPR does not cover posthumous personal data protection. Hence, it is imperative to refer once again to the French Digital Republic Act. In Article 40, the law provides guidelines a data subject should follow in his/her lifetime for the preservation, erasure and communication of personal data after death, failing which his/her successors are empowered to decide on what happens to the data upon his/her death – *iure heriditas,* on his/her behalf. Failure to comply with the instructions for storage, erasure and/or communication of a deceased person's personal data has dire implications for the processor and/or controller, including a fine of up to €100,000 per day of delay.[136]

Other good examples of law as a regulator of behaviour in cyberspace, with regards to posthumous person data protection, are: intellectual property law, laws regarding breach of confidence – medical health and legal advice, defamation law, and (US) right of publicity under state and case law.

The right of publicity – generally referred to as personality rights in Civil Law countries, empowers an individual to control the commercial exploitation of his/her name, image, likeness and other aspects of his/her personal identity.[137] The term "right of publicity" was coined by Judge Jerome Frank in Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.[138] Traditionally, like every right, the right of publicity ceased upon the death of the decedent, and estates were estopped from bringing actions before the courts in a bid to recover damages for the unauthorised use of the decedent's likeness.[139] Some US states have enacted statutes on posthumous right of publicity, they are: Alabama, California, Connecticut, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kentucky, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, Nevada, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington and Wisconsin. In Indiana, the right of publicity subsists 100 years after the death of the right holder – the longest posthumous personal data protection with a commercial interest anywhere in the world; in California, it is 70 years, in Kentucky, it is 50 years. However, these protections do not extend to appearances and/or uses in fiction and nonfiction entertainment. Also, the right of publicity covers only persons whose name, voice, photographs, signature and other aspects of their personal identity were of commercial value during their lifetime. The implication being that if Jane Doe – a relatively unknown woman who worked at a waitress in a downtown outlet of

[136] Article 46, France Digital Republic Act.
[137] *See supra* the cases of Mephisto; Dietrich.
[138] Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).
[139] Smolensky, *supra* note 39; *see also* Lugosi v. Universal Pictures, 603 P.2d 425 (Cal. 1979).

KFC's in California, were to pass on, her estate cannot claim the right of publicity to her image or likeness even if after her death she became renowned, say for heroism. This leaves the question of what happens when the decedent became famous upon death, Edgar Allan Poe, for e.g.? Will the courts recognise their posthumous right to the protection of their image and likeness?[140] Here, Charles Sykes assertion comes to mind:

> "But it is not the violations of the famous that make the battle over privacy the preeminent issue of the Information Age. It is the erosion of privacy in our everyday lives."[141]

Going by the Restatement (Third) of Unfair Competition, there are four elements which must be conjunctively present for a claim to right of publicity to prevail, they are: (1.) The defendant used the plaintiff's identity (2.) for the defendant's commercial (or other) advantage (3.) without the plaintiff's consent, (4.) causing injury. However, as shown by the court decision in Shaw Family Archives v. CMG Worldwide Inc. (2006), the laws on the right of publicity cannot apply retrospectively to cover decedents who did not have that right at the time of their death. This *ex post* nature of law is one of the most dominant criticisms of law as regulator of behaviour. Even as law satisfies the legitimacy principle necessary in every democratic society, its need to sanction after events and not work retrospectively makes it a somewhat lacking regulator for technology-induced behaviours.

4.3 Architecture as a regulator of behaviour in cyberspace

Lawrence Lessig asserts that "cyberspace has no nature, it has no particular architecture that cannot be changed. Its architecture is a function of its design – or [rather] its code."[142] This code changes over time as a necessity to follow the socio-technological developments of the time or because government or business propels it to change in a certain way – for example, Facebook's memorialisation policy.[143] This code functions in the form of software which a data subject can use to manage and/or determine the use or subsistence of his/her digital existence post-mortem.

According to Facebook's memorialisation policy, an account user has the option of choosing a legacy contact to manage the account – without having access to chats and posts except where authorised by the decedent to download his/her Facebook history, or have Facebook permanently delete the account.[144] Where an account user fails to choose a legacy contact, Facebook will have the account memorialised as soon as they become aware that the account user has passed on. Anybody on an account user's friend list can notify Facebook of the death of the account user, but the notification must be accompanied by a death certification, obituary or some other publication of note in order for Facebook to comply with the request. Facebook warns that memorialised accounts

---

[140] Smolensky asserts: "if an interest is incapable of being known after death, the law cannot protect it" (*supra* note 39, at page 772).
[141] Sykes (1999), *supra* note 10 at page 4.
[142] Lessig, Lawrence (1999). "The Law of the Horse: What Cyberlaw Might Teach". 113 Harv. L. Rev. 501.
[143] *Id*; *see also* Facebook. Memorialized Accounts. Available at: <https://www.facebook.com/help/1506822589577997> Accessed 05/10/2018.
[144] *Id.*

that don't have legacy contacts cannot be changed. The effects of memorialisation are: a.) the word "remembering" will be shown next to the user's name/profile; b.) where the user enabled friends – or anyone, where the privacy settings are set to public, to post on his/her "timeline", they can share memories on the memorialised timeline; c.) posts, photos, and videos shared by the account user will remain on Facebook, visible to the audience they were shared with; d.) the memorialised accounts ceases to feature in public spheres of Facebook, and even in private – such as birthday reminders; logins into the account will no longer be possible; and, e.) where an account user created a page and is the sole administrator of that page, the page will be deleted upon memorialisation of his/her user account.[145]

If the option to delete is chosen, Facebook will have the account on but not accessible for 30 days in case the request is regretted and withdrawn. If, after 30 days, the request is not withdrawn, Facebook will officially begin the process of deletion which can take up to 30 days to conclude.

For Twitter, the procedure is somewhat more straightforward: a request is made to Twitter's Trust and Safety Council accompanied by proof of death of the account user and proof of identity of the applicant and his/her ties to the account user whose death he notifies Twitter of. The request asks that the account of so so and so be deleted because they are dead. Twitter will examine the documents and take 30 days before they begin the process of deletion. When the process begins, it will take Twitter – like Facebook – 90 days to complete the deletion. Twitter also states in its Terms of Service that an account user cannot transfer his/her account to another person, because it issued the account user a non-negotiable, non-transferable license. As a result, an account will only continue to operate/exist if Twitter assumes that the user is still alive. There have been instances the decedent's family still had access to the account and posted tweets on behalf of the deceased, per his instructions.

Google's Inactive Account Manager follows the model of the Fiduciary Access to Digital Assets Act (Revised) which was addressed in Chapter 2 above. Google's Inactive Account Manager can be located on the settings page of one's Google Account. The feature enables the user to inform Google ahead of time what to do with his/her Gmail messages and personal data from other Google services – including Youtube, if the account becomes inactive for any reason and for a specified duration. The account user can choose to have his/her data deleted after three, six, nine or twelve months of inactivity. He/she can also select up to ten trusted contacts, and provide Google with their phone numbers, to receive data from some of or all of the following Google services: Blogger; Contacts and Circles; Drive; Gmail; Google+ Profiles, Pages and Streams; Picasa Web Albums; AdSense; Google Voice and YouTube. To verify that it is indeed the user who is initiating the Inactive Account Manager process, Google will send a text message to the mobile phone of the account user and an email to the secondary address he/she provided during registration. Google warns that deletion will affect all products/services associated with the account and the user will be unable to retrieve the username he/she once used for that account.

[145] *Id.*

This fiduciary-enabling feature of Google's Inactive Account Manager ensures that some of its services – for e.g. Blogger and YouTube, which generate income for the account users are easily incorporated in the deceased's estate planning, whether s/he died intestate or with a will. In contrast, Amazon whose platform also generates income for sellers with active accounts, customers and stored products in Amazon's warehouses does not have a likewise policy. Instead, the family, executor or personal representative of the decedent are encouraged to write Amazon via its Seller Support and notify them of the deceased's passing, then Amazon will decide what to do in line with the relevant jurisdiction and legal system.[146]

Interestingly, Google specifies in the Inactive Account Manager page that the account user can "decide if [their] account should be deleted" if inactive for too long. Thus, leaving no provision for presumption of death as a reason for the inactivity. This is interesting and problematic for posthumous data protection because, in so providing, Google inadvertently leaves a backdoor open for subsistence of accounts even when the user has passed away. Google has made clear that they know when an account is active or not; this they do by mapping log-ins, Android check-ins, Gmail usage and recent activities on MyActivity.[147] The prudent option would be for the service provider to stipulate a time limit on the inactivity, say thirty-six months, before it shuts down or freezes the account. Otherwise, what is the point in having an inactive account last "forever"? Dropbox – the cloud storage service provider, follows this prudent model. Dropbox will delete an account that has been inactive for fifteen. Before beginning the process of deletion, the service provider will send the account user a series of emails notifying them of the intention to delete the account and the reason behind it, i.e. inactivity. If the account user still wants to make use of the account, he/she must log into the account before the given deadline and the system will cancel the collated months of inactivity. Where the account user has passed away, Dropbox follows the Twitter model and asks for proof of death and ties with the deceased before proceeding to delete the account.[148] The company also has options for migration of account user's data, even posthumously, where the account user synced the application to their desktop windows.[149] However, this model of "protection" poses potential threats to the digital estate of a decedent as his successors-in-title will have no way of recovering the photos, videos, texts, etc. stored on Dropbox. Hence, the suggestion by some digital estate planners that people make a list of all accounts they use with their login details:

---

[146] Amazon, 2016. What Happens When an Account Holder Dies. Available at: <https://sellercentral.amazon.com/forums/t/what-happens-when-an-account-holder-dies/141219/6> Accessed 11/11/2018.
[147] Google. About Google Inactive Account Manager. Available at: <https://support.google.com/accounts/answer/3036546?hl=en > Accessed 28/10/2018.
[148] Dropbox. Help Center: How to Access the Dropbox Account of Someone Who Has Passed Away. Available at: <https://www.dropbox.com/help/security/access-account-of-someone-who-passed-away > Accessed 12/11/2018.
[149] *id*

usernames and passwords and leave same with trusted friends/family with clear instructions as to their use, management or deletion.[150]

On the other hand, the rationale for the silent policy of Google's with regards to leaving inactive accounts alone becomes clear when taking into consideration that some of their services – for e.g. YouTube and Blogger, are linked to Gmail accounts and are digital income generators managed as private businesses by individuals and legal entities, thus freezing an account or shutting it down because of the account user's inactivity will raise issues of interference with legitimate business interests and Google can be held civilly liable for lost income.

Furthermore, with the recent revelations about a security breach on Google+ and Google's plans to shut down the service, one wonders how Google proposes to resettle users of that service and deal with those inactive accounts without the Inactive Account Manager activated.[151] Would it arbitrarily shut down the service and with it the digital (after)lives of the account users? Only time will tell. This, however, highlights the problem of "digital rights": digital assets when unclaimed would most likely be erased by the company that controls them or they will continue to float in cyberspace long after the deceased's death.

4.4 The Market as regulator of behaviour in cyberspace

The market regulates behaviour through internal policies and rules of corporations which come to bear tremendously on the protection of (posthumous) personal data. These policies and rules are often – not always, embedded in the architecture of ICT products and services such that privacy is triggered and implemented by default and by design. Facebook and Google, being the kings of social media websites, were the first to come up with privacy policies that think beyond life. Facebook's memorialisation of accounts and legacy contact provisions and Google's Inactive Account Manager paved the way for (posthumous) personal data protection in the online world and motivated other social networking sites and cloud service providers to think in those terms. From Facebook to Google to LinkedIn to Twitter to Dropbox to Amazon to Adobe, the market continues to set standards for the protection of electronic content including personal data. The standards are implemented via the architecture of the software. For Facebook, Google, Twitter, etc., the standards are set via their privacy policies and implemented by precluding access without electronic security verifications. For Adobe's PDF, the standards are set by precluding alterations to documents without the maker's consent.

The Market in providing and encouraging posthumous data protection/privacy policies that enable data subjects to decide during their lifetime how and when to shut down their accounts – either in their lifetime or after death through fiduciaries who will

[150] Everplans. Digital Cheat Sheet: How To Create A Digital Estate Plan. <https://www.everplans.com/articles/digital-cheat-sheet-how-to-create-a-digital-estate-plan> Accessed 12/11/2018.
[151] The Washington Post. Google for months kept secret a bug that imperiled the personal data of Google+ users <https://www.washingtonpost.com/technology/2018/10/08/google-overhauls-privacy-rules-after-discovering-exposure-user-data/?noredirect=on&utm_term=.91df17732d80> Accessed 28/10/2018.

then manage the deceased's digital estate, inadvertently ensure that digital liabilities are avoided. Using Google's Inactive Account Manager as a model, imagine that James Gold subscribes to Netflix, BasicFit, Apple, TMobile, Anderzorg, Dropbox, Times, etc. on a monthly basis and pays via PayPal which accounts he created using his Gmail account. If the Gmail account is active, so will PayPal and Netflix and co; if there is money in the deceased's bank account to which the PayPal account is linked, then the subscriptions for the abovementioned services will subsist and be automatically paid for, even without the deceased's heirs' knowledge. However, whereby the Gmail account is shut down, all the other accounts will collapse, and the services will cease. The most such a business can do – especially in the case of yearly contracts, is initiate recovery of the debt owed, in which case they will learn of the deceased's passing and the termination of the contract by death.

4.5 Social norms as regulator of behaviour

This mode of regulation calls for a libertarian approach to personal data protection, ante mortem and post mortem, offline and online. Medical research relies heavily on cooperation of individuals to further science, it is imperative that the posthumous data protection of the individuals is at the forefront of policymaking. However, this is not a role solely for the institutions and governments, the data subjects themselves have the bulk of the decision-making. The most the institutions and governments can do is nudge the data subjects towards their preferred choices.[152] By encouraging data subjects to donate their personal/medical data – of their own free will while choosing the purposes and uses thereof, to clinics, research institutions, biobanks, we can begin to build a (social) norm where the determination of posthumous medical data lies with the data subjects themselves.

With advances in medical research and the reliance on genetic data to test and map genetic conditions, disorders and diseases such as Alzheimer's, sickle cell anaemia, etc., and establish family histories – sperm donor tracing, for e.g., issues of secondary use and data protection crop up.[153] Many medical data subjects assume that their data will be erased, or at least no longer be used upon their death, but this is not often the case. According to Shaw et al (2016), in many jurisdictions across the world posthumous medical data are still used for research as part of ethically approved research projects.[154] The Royal College of Physicians, for e.g., explains that archived medical data can be

[152] According to L. Reisch & C. Sunstein (2016), nudges are approaches to law and policy that maintain freedom of choice – à la Libertarianism, even as they steer the target audience in certain directions. Examples of how that is done include billboard advertisements and TV commercials.
[153] Taylor, M. 2012. Genetic Data and The Law: A Critical Perspective on Privacy Protection. Cambridge University Press, U.K. See also: Lunshof et al. 2008. "From Genetic Privacy to Open Privacy", in Science and Society, Vol. 9.
[154] Shaw et al, 2016. Data Donation After Death: A Proposal to Prevent the Waste of Medical Research Data, in: Science & Society, Science & Society. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4718407/> Accessed 05/11/2018.

used without consent as long as the research is not overly intrusive, the material/medical data are anonymised, and the subjects are not inconvenienced.[155]

The GDPR excludes posthumous personal data from its scope of application, however it provides for the (continued) processing of personal data of individuals for other purposes – with or without explicit consent of the individual,[156] if the purpose of such processing is for scientific research. This furthers the public interest theory that privacy is subject to the overriding interests of the public. This GDPR provision has implications for posthumous data protection where the individual dies during the subsistence of the processing for scientific research. In the case of genetic data, it has further implications for the living who are – by blood, related to the deceased. They can be identified via the genetic data through programs such as ancestry tracing and genome mapping. In the historic case of the HeLa cells,[157] a biopsy of a cancerous cervical tumour extracted from Henrietta Lacks was used to develop an immortal cell line, without her consent or knowledge, nor those of her family. Subsequent publications of the sequencing of the genome of the HeLa cells disclosed her identity and since then the Lacks family's genetic history remain public knowledge, their germline DNA can be used to draw medical inferences about them. Certainly, we have come a long since the 1950's and conceptions of medical privacy. I drew reference to the HeLa cells to make clear how worrisome undue protection of posthumous medical data is.

According to Shaw et al (2016) voluntary medical data donation will mitigate the problem of indiscriminate use of posthumous medical data as data subjects can choose which data to donate and which ones to have erased or anonymised.[158] To ensure that the family members of the deceased are not contacted for consent for one research purpose or the other, the medical data donated will be kept confidentially in a register managed by national or regional bodies whom researchers can apply to for access to the register.

4.6 Conclusion

These solutions – seen through the lens of Lessig's four modalities of constraints, can work together or singularly. When they work together, orchestrated to fall in sync, posthumous data protection will have a much higher chance of durability and acceptance. This is because where law works *ex post*, code/architecture, market and social norms work *ex ante*, thus minimising the chances of deviant behaviour. On the other hand, when they work singularly, the danger becomes that they clash with each other – Internet self-regulation versus law's legitimacy. Using the Facebook model as an example, the terms and conditions of service of Facebook – which is written into the architecture of the platform by way of username and password, stipulates that posthumous access to the account of a decedent is not transferable, even to heirs. This raises questions of laws supremacy, succession rights and contractual obligations. Should Facebook – the market,

---

[155] [No authors listed]. Research based on archived information and samples. Recommendations from the Royal College of Physicians Committee on Ethical Issues in Medicine. J R Coll Physicians Lond. 1999;33:264–266; see also Taylor (2012), supra note 135.
[156] Recital 158, GDPR.
[157] Jones, D.G. 2015. Genetic Privacy & The Use of Archival Human Material in Genetic Studies – Current Perspectives. Medicolegal & Bioethics. Vol. 5, Pp. 43-55.
[158] Shaw et al, *supra* note 154.

have this power to control inheritance rights and management of digital estates? If not, which constraint has or should have more say in that regard? Architecture – code, i.e., username and password? Law – privacy law, contract law, law of succession, reputation law? At this point, it appears that law, specifically contract law – working in tandem with the market, has more say. This is because law of succession and wills is catching up to changes in property/estate and legacy conceptions induced by technology, while the law of contract is still as fixed and stringent as ever. Edwards and Harbinja encapsulated this problem eloquently when they opined:

> "While Inheritance laws may have evolved to try to balance the interests of, say, parents and spouse of the deceased, or spouse and best friend, or even society (e.g *ultimushaeres* rules), contract is unlikely to think about the public good or what value society places on family ties".[159]

Furthermore, in EU countries, inheritance and property rights are matters of law for national legislators to deliberate upon and enact.[160] To have value, inheritance and property rights need to be enshrined in national laws.[161] But the issue remains that personal data as it is perceived generally is not property that can be inherited by descendants, hence Malgieri's argument for quasi-propertisation of personal data.[162] Especially now that data has become a valuable resource for the data driven economy wherein biometric data and genetic data can be used to accurately, automatically identify persons,[163] and predict and profile behaviours, traits and outcomes, not only of the deceased but also of the living whose lives connect to the former in some way(s).

Leaving the regulation of posthumous data protection to social norms has potentially harmful effects, as the current atmosphere of cyberspace being a place devoid of privacy is counterproductive. The personal data can be abusively interfered with, financially profited from without any benefit to the data subject,[164] the data can be used to exploit the grief and emotions of their descendants,[165] the health or genetic data of the decedent may be used unlawfully to determine the health or genetic data of the descendants.[166] Moreover, personal data has become an information good with powerful ties that bind customers/consumers and companies. The economic value of personal data to corporations, institutions and governments makes its protection (solely) through expectations of goodwill and good behaviour unfeasible. Being that the information

---

[159] Edwards & Harbinja, *supra* note 17, at page 120.
[160] *Id.*
[161] Malgieri 2016B, *supra* note 34, at page 13.
[162] Malgieri 2018, *supra* note 19.
[163] Biometrics Research Group, N.D. "What is Biometrics?". Available at: <http://biometrics.cse.msu.edu/info/index.html> Accessed 27/10/2018.
[164] In Moore v. Regents of University of California, the Supreme Court of California held that a patient does not have property interest in his cells, as the cells were common to all men.
[165] A technology company, Luka, has created an app called "griefbot" which mirrors the behaviour of a decedent using their social media profiles and other data supplied by their loved ones. *See:* The Sun. 2018. TEXT IN PEACE How 'griefbots' let us chat to the dead from our phones… Available at: <https://www.thesun.co.uk/tech/5681776/griefbots-messages-dead-roman-mazurenko/>; To use a "griefbot", see www.eterni.me.
[166] Malgieri 2018, *supra* note 19.

industry has immeasurable clout in the current economic climate that relies heavily on digital technology to generate wealth, they have strong claims to personal data on cyberspace.[167]

[167] Malgieri 2016A, *supra* note 54.

Chapter 5 Conclusion

> "The life of the dead is placed in the memory of the living."
>
> – Marcus Tullius Cicero

The nature of social media ensures that humans via their Facebook posts, Wordpress, Blogger blogposts, tweets, Instagram photos and videos, and YouTube vlogs, will exist "forever" in digital form. When examined from the angle of preservation of historical and bibliographic accounts, these digital afterlives are incredible resources for public and private consumption – many a grandchild will cherish a chronicle of their grandparent's life, a sort of memoir that outlines social and political thoughts. However, when viewed from the angle of privacy – "the right to be let alone" and the many harms that can and do arise from abuse of a decedent's personal data, these digital afterlives emit a clarion call for a preservation of the dignity, privacy and reputation of the deceased. It reflects a need for the protection of posthumous personal data protection, not just on cyberspace but in the physical world. Yet, the determination of digital afterlives is not absolute nor is it straightforward. Many nuances and interests, public and private, come into play, with the principal question being: who should protect these data and how?

At European Union level, a call for posthumous personal data will not be welcomed and answered by all Member States as each state has its own unique history and traditional beliefs upon which its legal system is built. Where some Member States, Germany and France, for instance, will welcome a uniform regulation of posthumous data protection, others, for e.g., the United Kingdom, will consider it an affront on their legal system which explicitly disassociates the dead from having autonomous rights. Thus, a posthumous data protection framework under EU law is not necessarily needed. Instead, Member States should be encouraged to promote and protect posthumous personal data, either through legislations, case law, or encouragement of co-regulation with ISPs.

Those Member States – Italy and Bulgaria for instance, whose legal systems do not prohibit posthumous personal data protection would do well to follow the path of France's Digital Republic Act, particularly those provisions which make it possible for a decedent to determine while still alive what happens to his/her personal data upon his/her death. Thereby reducing the problem of an autonomous data subject when issues of posthumous personal data protection crop up.

However, law as was discussed in Chapter 4 is not the only means of regulating behaviour. The Market, the architecture (read: technology/code), and social norms have equally important roles to play. Those roles should be played in conjunction with state laws/policies to ensure their efficacy, legitimacy and transparency. This can be done in any of the following ways:

- The state could require ISPs to produce and market standardised technological mechanisms – as part of their services, for the preservation, deletion, inheritance or donation of digital assets.
- The state could mitigate or prohibit the proliferation of ISPs with "free" service models who rely on data mining and sale of personal data for profit, thereby requiring data subjects to pay for the services. This will incentivise ISPs to compete with one another to provide the best service possible to users, including the posthumous protection of the personal data they control and process and work to ensure that the interests of data subjects are taken into consideration when modelling software applications.
- The state could legally place the burden of the protection of posthumous data protection on data subjects by requiring them to plan their digital estates ante mortem, or risk forfeiting of same to the state. Using Google's Inactive Account Manager as an example, an inactive account without a manager which has been inactive for the legally stipulated period for presumption of human death will have all digital assets in it or connected to it ceded to the state. A somewhat illiberal approach, but this will incentivise data subjects to plan their digital estates *ante mortem* thereby protecting their personal data posthumously.

Summarily, a hybrid form of co-regulation – the interactive cooperation of Lessig's four modalities of regulation, is a promising alternative to the establishment of effective protection of posthumous personal data protection.

Bibliography

Books & Journal Articles

Buitelaar,J. C. 2017. Post-mortem privacy and informational self-determination. Ethics and Information Technology, Vol 19 pp.129-142.

Cesare, N. & Brandstad, J. 2017. Mourning and Memory in The Twittersphere. Journal Mortality: Promoting the Interdisciplinary Study of Death and Dying. Volume 23 Issue 1, Pp. 82-97.

Edwards, L. & Harbinja, E. 2013. Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. Cardozo Arts & Entertainment Law Journal, Vol. 32, No. 1, 2013.

Harbinja, E. 2013. Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives? Scripted, a Journal of Law, Technology & Society.

Hertogen, A. 2015. Letting Lotus Bloom. European Journal of International Law, Volume 26, Issue 4, Pages 901–926.

Hutchinson, T. 2017. "Doctrinal Research: Researching the Jury", in: Research Methods in Law, Watkins, D. & Burton, M. 2017 (eds.). Routledge, U.K.

Immanuel Kant. 2017. The Ethics of Immanuel Kant: Metaphysics of Morals – Philosophy of Law & the Doctrine of Virtue. Musaicum Books.

Jones, D.G. 2015. Genetic Privacy & The Use of Archival Human Material in Genetic Studies – Current Perspectives. Medicolegal & Bioethics. Vol. 5, Pp. 43-55.

Kirley, Elizabeth Anne. 2015. Reputational Privacy and the Internet: A Matter for Law? *PhD Dissertations*. 8. Available at: <https://digitalcommons.osgoode.yorku.ca/phd/8 > Accessed 30/09/2018.

Kozyris, P. J. 2007. Regulating Internet Abuses: Invasion of Privacy. Kluwer Law International. The Netherlands.

Krutzinna, J., Taddeo, M. & Floridi, L. 2018. Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data. Available at SSRN: <https://ssrn.com/abstract=3177989 > Accessed 28/08/2018.

Lessig, L. 1999. Code and Other Laws of Cyberspace. Basic Books. New York, USA.

Lessig, L. 1998. The Laws of Cyberspace. Available at: <https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf> Accessed 05/10/2018.

Levinson, P. 2009. New New Media. Pearson, USA.

Lomio, J., Spang-Hanssen, H., & Wilson, G. 2011. Legal Research Methods in a Modern World. Djof Forlag, Denmark.

Lunshof et al. 2008. "From Genetic Privacy to Open Privacy", in Science and Society, Vol. 9.

Malgieri, Gianclaudio. 2018. Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. Privacy in Germany - PinG, n. 4, 2016, 133 ff. Available at SSRN: < https://ssrn.com/abstract=2916058 > Accessed 30/09/2018.

Malgieri, Gianclaudio, R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions (March 30, 2018). Data Protection and Privacy: The Internet of Bodies, edited by Ronald Leenes, Rosamunde van Brackel, Serge Gutwirth & Paul De Hert (Brussels, Hart, 2018). Available at SSRN: <https://ssrn.com/abstract=3185249> Accessed 01/10/2018

Malgieri, Gianclaudio, 'Ownership' of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution? (November 20, 2016). Journal of Internet Law, Vol. 20, n.5, November 2016. Available at SSRN: < https://ssrn.com/abstract=2916079 > Accessed 30/09/2018.

Mann, S. & Ferenbok, J. 2013. New Media and the power politics of sousveillance in a surveillance-dominated world. Surveillance Futures, Vol. 11 No. 1/2.

McConville, M. & Chui, W. 2007. Research Methods for Law. Edinburg University Press, U.K.

Mill, J.S. 1859. On Liberty. Available at: <https://eet.pixel-online.org/files/etranslation/original/Mill,%20On%20Liberty.pdf> Accessed 28/10/2018.

Newman, S. 2011. The Development of Copyright & Moral Rights in the European Legal System. SSRN.

[No authors listed]. Research based on archived information and samples. Recommendations from the Royal College of Physicians Committee on Ethical Issues in Medicine. J R Coll Physicians Lond. 1999; 33:264–266.

Park, S. and Sánchez Abril, P. 2016. Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights. American Business Law Journal,53(3), 537-598.

Post, R. 2001. Three Concepts of Privacy. Faculty Scholarship Series, Vol. 185.

Purtova, N. 2015. The Illusion of Personal Data as No One's Property. Journal of Law, Innovation & Technology. Vol. 7. Issue 1, Pp.83-111 at p. 83.

Rosler, H. 2008. Dignitarian Posthumous Personality Rights – An Analysis of U.S. & Germany Constitutional and Tort Law. Berkeley Journal of International Law. Vol. 26. No. 153.

Shaw et al, 2016. Data Donation After Death: A Proposal to Prevent the Waste of Medical Research Data, in: Science & Society, Science & Society. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4718407/> Accessed 05/11/2018.

Shu, N. 2015. Protecting Privacy after Death. Northwestern Journal of Technology and Intellectual Property Law, Vol. 13 No. 2.

Smolensky, K. R. 2009. Rights of the Dead. Hofstra Law Review, Vol. 37, Issue 3.

Solove, D. 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review.

Solove, D. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review 745.

Sperling, D. 2008. Posthumous Interests: Ethical and Ethical Considerations. Cambridge University Press, U.K.

Sykes, C. J. 1999. The End of Privacy. St. Martin's Press, New York.

Taylor, M. 2012. Genetic Data and The Law: A Critical Perspective on Privacy Protection. Cambridge University Press, U.K.

Van der Sloot, B. 2016. "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities", in: Data Protection on the Move: current developments in ICT and privacy/data protection. Pp. 411-436. Springer, Dordrecht.

Warren & Brandeis. 1890. The Right to Privacy. Harvard Law Review. Vol. IV, No. 5.

Zhao, S. B. 2017. "Exposure and Concealment in Digitalized Public Spaces", in: B. C. Newell, T. Timan, & B-J. Koops (Eds.), Privacy in Public Spaces: Conceptual and Regulatory Challenges. Edward Elgar Publishing.

Zhao, S. B. 2016. Posthumous Defamation and Posthumous Privacy Cases in the Digital Age. Savannah Law Review Vol. 3, No. 1.

Zhao, S. B. 2014. Legal Cases on Posthumous Reputation and Posthumous Privacy: History Censorship, Law, Politics and Culture. Syracuse Journal of International Law and Commerce, Vol. 42, No. 1 [2014], Art. 4.

Zhao, S. B. 2014. Posthumous Reputation and Posthumous Privacy in China: The Dead, the Law, and Social Transition. Brooklyn Journal of International Law, Vol. 39 Issue 1.

Legislation

California Code, Civil Code.

Charter of Fundamental Rights of The European Union (2000/C 364/01).

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01. Web. < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT > Accessed: 16/03/2018.

General Penal Code, Ireland.

German Penal Code (*StGB*). Translation provided by Prof. Dr. Michael Bohlander. Available at: < https://www.gesetze-im-internet.de/englisch_stgb/index.html > Accessed 01/10/2018.

German Civil Code (*BGB*). Translation provided by the Langenscheidt Translation Service. Available at: < https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p3489 > Accessed 01/10/2018.

Italian Civil Code.

Loi n°2016-1321 pour une République numérique. Available at: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id > Accessed 3/11/2018.

Personal Data Protection Act, Bulgaria.

Personal Data Protection Act, Estonia.

The General Data Protection Regulation (EU) 2016/679.

Case Law

BVerfGE 75, 369 1 BvR 313/85. Translation provided by Nomos Verlagsgesellschaft. Available at: https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=634. Accessed 01/10/2018.

1 BvR 400/51; translation supplied by: Tony Weir, University of Texas at Austin. Available at: <https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=1369> Accessed 30/09/2018.

BvR 240/04. Translation provided by Raymond Youngs, University of Texas at Austin. Available at: < https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=1499 > Accessed 30/09/2018.

Couderc & Hatchette Filipacchi Associates v. France. (ECtHR) Application No.40454/07

Estate of Kresten Filtenborg Mortensen v. Denmark. (ECtHR) Application no. 1338/03.

Flynn v. Higham, 149 Cal.App.3d 677 (1983).

Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).

Hughes v. New England Newspaper Publishing Co. 312 Mass. 178 (1942).

JCP 1977. II. 22894. Translation provided by Tony Wier. Available at: <https://law.utexas.edu/transnational/foreign-law-translations/french/case.php?id=1240> Accessed 01/10/2018.

Koch v. Germany. (ECtHR) Application no. 497/09.

Lugosi v. Universal Pictures, 603 P.2d 425 (Cal. 1979).

Rose et al. v. Daily Mirror, Inc., 20 N. Y. S.(2d) 315 (App. Div. 2d Dept. 1940).

Volker und Markus Scheke GbR and Hartmut Eiffert v. Land Hessen. (CJEU) C-92/09 & C-93/09.

Others

Angelo, M. 2009. "You are what Google says you are". Wired, 12 Nov. 2009. Available at: < https://www.wired.com/2009/02/you-are-what-go/ > Accessed 07/05/2018.

Amazon, 2016. What Happens When an Account Holder Dies. Available at: <https://sellercentral.amazon.com/forums/t/what-happens-when-an-account-holder-dies/141219/6> Accessed 11/11/2018.

Biometrics Research Group, N.D. "What is Biometrics?". Available at: <http://biometrics.cse.msu.edu/info/index.html> Accessed 27/10/2018.

DLA Piper, 2016. France adopts Law for a Digital Republic: key data provisions are a jump-start on the GDPR. Available at: < https://www.dlapiper.com/en/us/insights/publications/2016/11/france-adopts-law-for-a-digital-republic/ > Accessed 30/09/2018.

Dreyfus. 2017. Part 3: French Digital Republic Law – right to privacy. Available at: <http://www.dreyfus.fr/en/new-technologies/part-3-french-digital-republic-law-right-to-privacy/> Accessed 01/10/2018.

Dropbox. Help Center: How to Access the Dropbox Account of Someone Who Has Passed Away. Available at: <https://www.dropbox.com/help/security/access-account-of-someone-who-passed-away > Accessed 12/11/2018.

Everplans, n.d. Digital Cheat Sheet: How To Create A Digital Estate Plan. <https://www.everplans.com/articles/digital-cheat-sheet-how-to-create-a-digital-estate-plan> Accessed 12/11/2018.

Facebook, n.d. Memorialized Accounts. Available at: <https://www.facebook.com/help/1506822589577997> Accessed 05/10/2018.

FieldFisher. 2016. France Adopts Digital Republic Law. Available at: <https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law> Accessed 01/10/2018.

Google. About Google Inactive Account Manager. Available at: <https://support.google.com/accounts/answer/3036546?hl=en > Accessed 28/10/2018.

Hovde, A.L.L. 2016. Grief 2.0: Grieving in an Online World. Available at: <https://www.duo.uio.no/bitstream/handle/10852/52544/Hovde-Master-2016.pdf?sequence=5> Accessed 28/10/2018.

Splinter. These are The Most Influential Dead People on Twitter. Available at: <https://splinternews.com/these-are-the-most-influential-dead-people-on-twitter-1793855156 > Accessed 28/10/2018.

The Sun. 2018. TEXT IN PEACE How 'griefbots' let us chat to the dead from our phones… Available at: <https://www.thesun.co.uk/tech/5681776/griefbots-messages-dead-roman-mazurenko/>

The Washington Post. Google for months kept secret a bug that imperiled the personal data of Google+ users <https://www.washingtonpost.com/technology/2018/10/08/google-overhauls-privacy-rules-after-discovering-exposure-user-data/?noredirect=on&utm_term=.91df17732d80> Accessed 28/10/2018.

Thoren-Peden, D.S & Meyer, C.D. 2018. Data Protection 2018: USA. Available at: < https://www.pillsburylaw.com/en/news-and-insights/data-protection-2018-usa.html > Accessed 30/09/2018

Twitter. Privacy Form | Twitter Help Center. < https://help.twitter.com/forms/privacy > Accessed 06/04/2018.

What is a legacy contact and what can they do? | Facebook Help Centre | Facebook Web. <https://www.facebook.com/help/1568013990080948 > Accessed: 16/03/2018.

What is Personal Data? |European Commission (n.d.) |Web. < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en > Accessed 21/06/2018.

World Intellectual Property Organisation (WIPO). 2016. Understanding Copyright and Related Rights. Available at: < http://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf > Accessed 01/10/2018.