Post-Mortem Data Protection in the Age of Big Data and its Threat to Personal Autonomy

Tilburg Institute for Law, Technology and Society (TILT)
LL.M. Law and Technology (2013 – 2014)

Roxane Farrugia
ANR: 536715 / EMP: 1259253

Thesis Supervisor: Dr N. N. Purtova
Second Reader: Prof. E. J. Koops
August 2014

Table of Contents

Chapter IV - Is the Distinction between Data of Deceased and Living Individuals Justified?

Introduction

1. BACKGROUND AND SIGNIFICANCE

This thesis aims to explore whether, in light of the age of big data and the threat it poses to individuals' personal autonomy, there exists a need for post-mortem data protection. Specifically, the author seeks to examine whether data used in big data analytics also data pertaining to deceased persons. If this is the case, it would mean that the concerns attached to big data arise from the processing of data pertaining to both living and deceased individuals. The aim of data protection is to safeguard individuals from harms which may ensue from data processing[1], particularly the invasion of privacy and the violation of values attributed to it, such as personal autonomy[2]. In light of this, the author questions whether the fact that the data subject is living or deceased should determine whether protection is afforded over his data.

2. RESEARCH QUESTION AND ROADMAP

The central research question to be addressed throughout this thesis shall be as follows:

> *In the age of big data and its threat to personal autonomy, should it matter if the data pertains to living or deceased individuals for the purposes of data protection?*

In order to arrive at an answer to this research question, the author has formulated the following roadmap:

[1] P. De Hert and S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E. Claes, A. Duff and S. Gutwirth (eds.), Privacy and Criminal Law (Antwerp/Oxford, Intersentia, 2006) 61 – 104.

[2] The principle of personal autonomy has been deemed by the European Court of Human Rights to fall within the scope of the right to private life. See *Pretty v The United Kingdom* App No 2346/02 (ECtHR, 29 April 2002).

1. The rationale of data protection and its relevance to personal autonomy – the author shall start off by looking into how personal autonomy forms part of the rationale of data protection. The first chapter will deal with basic questions: What is the purpose of data protection? Why do individuals need it? How does data protection benefit society as a whole?
2. The risks of big data – the author shall then move on to assessing the concerns that have arisen with the advent of big data. How do big data analytics affect individuals and society? Can they have negative consequences? Once again, specific reference will be made to personal autonomy – how does big data pose a risk to personal autonomy?
3. The longevity of data – in the second chapter the author shall delve into the lifetime of data in the big data processing pool. When does data stop being processed by big data companies? In particular, is data pertaining to an individual still processed for the purpose of big data analytics after his death?
4. Data protection law and data pertaining to deceased persons – in the third chapter the author shall assess how data protection law deals with the longevity of data. Specifically, does data continue to benefit from protection after the death of the data subject?
5. Post-mortem data protection – in light of the answers to the aforementioned questions, the fourth chapter shall then explore the notion of post-mortem data protection. Should data protection law distinguish between data of living and deceased individuals in its applicability?

3. LITERATURE REVIEW

The treatment to be afforded to data pertaining to deceased individuals has become a topic of interest on an international scale in recent years[3]. Presently, literature on this topic does not tackle post-mortem data protection in light of the advent of big data and the risks that it presents. Primary areas of debate tend to relate more to the transmission of a deceased's digital assets and his "digital self"[4]; and the issue of access to a deceased person's data[5]. The aspect of control over one's data after death seems to interest many authors in the field, with questions like 'what happens to my Facebook account after I die?' and 'who will own my email when I pass away?' being very popular[6].

[3] The earliest literature found by the author on this subject dates back to 2005 (See R. Herold, *Is There Privacy Beyond Death?* (CSI Alert, March 2005)); however the majority of works on this topic were written from 2013 onwards (See for instance E. Harbinja, *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could be the Potential Alternatives?* (Scripted, Vol. 10 Issue 1, April 2013); L. Edwards and E. Harbinja, *Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World* (Cardozo Arts & Entertainment Law Journal, Vol. 32 No. 1, November 2013); and J. Bikker, *Disaster Victim Identification in the Information Age: The Use of Personal Data, Post-Mortem Privacy and the Rights of the Victim's Relatives* (Scripted, Vol. 10 Issue 1, 2013)).

[4] See for instance, L. Edwards and E. Harbinja, *"What happens to my Facebook profile when I die?": Legal Issues around Transmission of Digital Assets on Death*, 21st February 2013 accessed via http://ssrn.com/abstract=2222163 on 11th November 2013. Current Ph. D. research being conducted by Harbinja also revolves around 'Legal Aspects of Transmission of Digital Assets on Death', see http://www.strath.ac.uk/humanities/courses/gradschool/studentprofiles/edinaharbinja/ accessed on 29th June 2014 for more details.

[5] For instance, Molly Wilkens discusses whether privacy and security applied in respect of financial information during an individual's life can constitute a barrier to access of same information by an estate executor after his death. See M. Wilkens, *Privacy and Security during Life, Access after Death: Are They Mutually Exclusive?* (Hastings Law Journal, Vol. 62, March 2011) 1037 – 1064.

[6] For instance, the Irish Research Council launched a research project with the aim of providing "clear policy foundations for Internet-based service providers to define their obligations regarding the accounts of the deceased…underpinning the regulation and control of the digital/virtual-self following death". See D. McCallig, *The Law of Digital Remains*, accessed via http://research.ie/intro_slide/law-digital-remains on 31st January 2014. See also D. McCallig, *Facebook after death: an evolving policy in a social network* (International Journal of Law and Information Technology, 2013) 1 – 34.

The topic of post-mortem data protection has also been approached from a medical/health data perspective. For instance, Tasse[7] questions what should be done with data consisting of research results which are only returned after the participant's death. Bongers[8], on the other hand, delves into the rights and entitlements of the survivors of a deceased individual and discusses whether inspection of medical records of the deceased can be conducted by relatives having a legitimate interest. Other authors have taken on a "privacy of death" view[9]. In particular, Bikker[10] focuses on disasters and the publicity of victims that comes with them. He explains how the availability of hand-held mobile technology and internet access enable the public to act as journalists and publicize graphic images and information about the victims of disasters shortly after they happen[11]. Bikker also delves into the concept of "post-mortem relational privacy", analyzing the "*fine line between privacy, decency and 'the right to know*'"[12]. He raises awareness about the tug-of-war between the will of victims' survivors to disclose information about them for the purposes of tracing and identifying victims and the invasion of victims' privacy that may occur as a result of such disclosure[13].

[7] A. Tasse, *The Return of Results of Deceased Research Participants* (Journal of Law, Medicine and Ethics, Winter 2011) 621 – 630.
[8] L. M. H. Bongers, *Disclosure of Medical Data to Relatives after the Patient's Death: Recent Legal Developments with respect to Relatives' Entitlements in the Netherlands* (European Journal of Health Law 18, 2011) 255 – 275.
[9] See D. Hamill, *The Privacy of Death on the Internet: A Legitimate Matter of Public Concern or Morbid Curiosity* (Journal of Civil Rights and Economic Development, Vol. 25, 2011) 833 – 871 and C. Calvert, *The Privacy of Death: An Emergent Jurisprudence and Legal Rebuke to Media Exploitation and a Voyeuristic Culture* (Digital Commons at Loyola Marymount University and Loyola Law School, 2006) 133 - 169.
[10] J. Bikker, *Disaster Victim Identification in the Information Age: The Use of Personal Data, Post-Mortem Privacy and the Rights of the Victim's Relatives* (Scripted, Vol. 10, Issue 1, 2013) 57 – 76.
[11] Ibid 61.
[12] Ibid 61.
[13] Ibid (n 10) 65.

Issues such as personality rights[14], publicity rights[15] and rights of the dead in general[16] have also been the central topic of a number of works related to data of deceased individuals. "[D]*ignity and autonomy* [have been held to] *play a large role in the granting of posthumous rights by lawmakers*"[17], such as the right to post-mortem privacy or post-mortem data protection. Harbinja[18] tackles the topic from the perspective of identifying what happens to the deceased's data and deliberating whether deceased persons should be entitled to benefit from post-mortem data protection in order to maintain a degree of privacy even after death[19].

As can be seen from the above, for the most part, existing literature about post-mortem data protection does not consider the issue in light of the recent developments in data analytics, including big data analytics, but rather revolves around the notion of control over data. The EU data protection regime in general is largely "*connected to the idea of informational self-determination both on the level of objectives and specific control rights of the data subject*"[20]. Enforcement of data protection rules is achieved through these control rights to data subjects – the right to access, the right to information, the right to rectify personal data, etc[21]. Consent is also set up to play a crucial role as the main means for obtaining permission and establishing the conditions for the processing of personal data[22].

[14] See H. Rosler, *Dignitarian Posthumous Personality Rights – An Analysis of U.S. and German Constitutional and Tort Law* (Berkeley Journal of International Law, Vol. 26, Issue 1, 2008) 153 – 205.
[15] See A. Hicks, *The Right to Publicity after Death: Postmortem Personality Rights in Washington in the Wake of Experience Hendrix v. HendrixLicensing.com* (Seattle University Law Review, Vol. 36, 2012) 275 – 297.
[16] See K. R. Smolensky, *Rights of the Dead* (Hofstra Law Review, Vol. 37, 2009) 763 – 803.
[17] Ibid 802.
[18] E. Harbinja, *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?* (Scripted, Vol. 10, Issue 1, April 2013) 19 – 38.
[19] Ibid 22.
[20] N. Purtova, *Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table…and back on again?* (Computer Law and Security Review, December 2013) 6.
[21] See Ibid 9 – 11.
[22] See Articles 7 (a), 8 (2) (a), 8 (2) (d), 26 (1) (a) of the Data Protection Directive.

However more recent literature[23] contends that control and consent are wavering in their significance and effectiveness as tools for the enforcement of data protection rules. For instance Solove[24], referring to informational self-determination and control mechanisms in data protection as "privacy self-management", argues that "*privacy self-management cannot achieve the goals demanded of it, and it has been pushed beyond its limits*"[25]. Moerel[26] further argues that the use of a consent requirement for the granting of control to the data subject has become "*subject to 'routinisation' and therefore meaningless*"[27]. Kuner[28] presents a number of instances where consent proves to be an unreliable tool for establishing a ground to process data. For instance, in an e-commerce set-up, consent is very often given by means of tick boxes or the acceptance of lengthy and complicated privacy policies. Individuals are generally not fully aware of and do not understand what they are consenting to[29], rendering the act of giving consent to constitute a mere formality bearing no actual significance. Furthermore, in the majority of cases, providing consent is the only option made available to the individual if he wants to make use of a particular commodity[30].

[23] See D. J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma* (Harvard Law Review Vol. 126, 2013) 1880 – 1903; Ibid (n 15) 24; and Ibid (n 20) 11 – 12.
[24] D. J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma* (Harvard Law Review Vol. 126, 2013)
[25] Ibid 1903.
[26] L. Moerel, *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*, Lecture delivered during the public acceptance of the appointment of professor of Global ICT Law at Tilburg University, 14th February 2014.
[27] Ibid.
[28] C. Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2nd ed., 2007),
[29] Ibid 68.
[30] Ibid (n 26).

In light of the above, the author has opted to stray away from notions as are the transmission, access, disclosure, and ultimately the control of data. The focus of this thesis shall rather be on assessing whether there exist reasons to discriminate between data of living and deceased individuals when applying data protection in light of the threats to personal autonomy that are brought about by big data analytics.

4. METHODOLOGY

4.1 Research Methodology

Doctrinal legal research shall be conducted in order to address the research question forming the basis of this thesis. Doctrinal legal research is concerned with the formulation of legal doctrines through interpretative and qualitative analysis of legal rules[31]. Research to be conducted will be desk-based, i.e. by locating applicable legislation, case-law and relevant literature. The research method chosen will be applied using a problem-based approach: assembling facts; identifying legal issues; analyzing issues with a view to searching for potential solutions; and arriving at a tentative conclusion[32]. In assembling the facts for the purposes of identifying legal issues, the author shall conduct mainly an internal (by analyzing the texts of the law[33]), but to some extent also an external (by analyzing how the law is applied in society[34]) research methodology.

[31] P. Chynoweth, 'Legal Research' in A. Knight and L. Ruddock (ed.), 'Advanced Research Methods in the Built Environment' (Blackwell Publishing Ltd, 2008).
[32] See T. Hutchinson and N. Duncan, *Defining What We Do – Doctrinal Legal Research* accessed via http://www.scribd.com/doc/191621387/Hitchinson-and-Duncan on 29th June 2014.
[33] Ibid.
[34] Ibid.

4.2 Scope and Limitation

The scope of this thesis is to look into the threats posed by the advent of big data, particularly the threat to personal autonomy, with a view to assessing whether this gives rise to a need for post-mortem data protection. It shall however be beyond the scope of this thesis to delve into the efficacy of the data protection regime in addressing and preventing the harms that big data may bring about.

The jurisdictional scope of this thesis shall be restricted to the legal system of the European Union (EU). Any references made to literature, legislation, policies or other material originating from jurisdictions outside of the EU shall be solely for illustration or comparison purposes Notwithstanding this, in an effort to understand the approach being taken by individual Member States in regard to the treatment of data in a post-mortem stage, the author has chosen to briefly assess a few national data protection laws.

For the purposes of assessing data protection legislation within the EU, the author has chosen to focus on the Data Protection Directive[35]. However, in light of the upcoming revamp in this area, the proposed General Data Protection Regulation[36] shall also be examined. The author shall not

[35] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[36] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

delve into the Convention on Data Protection[37] since the Data Protection Directive is intended to give substance and to amplify the provisions of this Convention[38].

5. CHAPTER OVERVIEW

The first chapter of this thesis is intended to provide some background information in order to set the context. In particular, it shall delve briefly into the rationale of data protection and some of the concerns attached to the advent of big data. The second chapter looks into the duration for which data is processed for the purposes of big data analytics. This chapter seeks to identify whether data pertaining to deceased individuals is used in the same manner as data of living individuals in big data analytics. In order to do so, the author shall analyse the practices and policies of a number of data controllers involved in big data analytics with a view to identifying whether treatment of data varies depending on whether the person it pertains to is living or deceased.

The third chapter is aimed at identifying whether the current EU data protection regime distinguishes between data of living and deceased individuals in the application of its rules. In light of expected changes to the regime, the text of the proposed General Data Protection Regulation, shall also be assessed. Having due regard to the findings of the previous chapters, the fourth chapter shall assess whether a distinction should be made by data protection law between data pertaining to living and deceased individuals for the purposes of according protection. In this regard the

[37] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28th January 1981.

[38] Recital 11 of the Data Protection Directive states that "the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

author shall provide arguments in favour and against post-mortem data protection and briefly discuss a couple of options for the way forward. The author will close off this thesis with some final thoughts in the concluding chapter.

Chapter I

Understanding the Context – Big Data and the Threat to Personal Autonomy

1. SCOPE AND PURPOSE

In order to adequately address the issue at the heart of the central research question, we must first set the scene and properly understand the context from which the issue has arisen. Throughout this chapter the author aims to provide a brief account on the main elements which form the background to the central research question. In particular, we shall look into the rationale of data protection to better understand why the protection of individuals' personal autonomy is a priority on the agenda of data protection. The author also seeks to explore some concerns attached to the notion of big data and big data analytics. Specifically, we shall look at how big data can pose a threat to personal autonomy.

2. THE RATIONALE OF DATA PROTECTION – WHY PERSONAL AUTONOMY MAKES IT ONTO THE AGENDA

The data subject constantly finds himself in situations where he needs to give up his data to third parties, be it in the public or private sector[39]. This inherently places the data subject in a weaker position than the data controller. Data protection aims to balance out the power of the data controller by giving the data subject a degree of control over his data and devising regulations to promote transparency and accountability on the part of data controllers[40]. Data protection also seeks to safeguard individuals' rights and freedoms insofar as these may be adversely affected by the processing of data[41]. Notwithstanding this, data protection is not prohibitive in nature – it

[39] Ibid (n 1).
[40] Ibid (n 1).
[41] F. Coudert, *Towards a New Generation of CCTV Networks: Erosion of Data Protection Safeguards?* (Computer Law and Security Review, 25, 2009) 148.

acknowledges that there exists a need for the processing of personal data but also gives importance to the prevention of harms which may ensue therefrom[42]. It does so by regulating the manner in which data is processed by data controllers[43].

The prevention of privacy invasion in the course of data processing is at the core of the scope of data protection. However there exist other values that emerge from the notion of privacy which are also on the agenda of data protection[44]. In particular, privacy promotes liberty, autonomy, selfhood and human relations, all of which are essential for a free society[45] and may be threatened through the processing of data. For instance, personalization services that may ensue from data processing are capable of putting individuals' personal autonomy and self-determination at risk when they are used to manipulate human behaviour[46]. Autonomy has been defined as "*the fundamental right of individuals to shape their own future through voluntary action."*[47] It is hence not solely an individual value, but also constitutes a central value for a functioning democracy[48]. On this note, Rouvroy and Poullet[49] argue that "*individual autonomy and deliberative democracy presuppose a series of rights and liberties allowing individuals to spend a life characterized as*

[42] Ibid (n 1).
[43] Ibid (n 1).
[44] L. Bygrave, *The Place of Privacy in Data Protection Law* (UNSW Law Journal, Vol. 24 no. 1, 2001) 281.
[45] K. Laas-Mikko and M. Sutrop, *How do Violations of Privacy and Moral Autonomy Threaten the Basis of our Democracy?* (TRAMES: A Journal of the Humanities & Social Science, Vol. 16 Issue 4, 2012) 370.
[46] J. E. J. Prins, 'Digital Diversity: Protecting Identities instead of Individual Data' in L. Mommers (ed.) Het Binnenste Buiten: Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout Schmidt (Leiden University, 2010) 297.
[47] W. H. van Boom and A. Ogus, *Introducing, Defining and Balancing 'Autonomy v. Paternalism'* (Erasmus Law Review, Vol. 3 Issue no. 2, 2010).
[48] Ibid (n 45) 378.
[49] A. Rouvroy and Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (eds.) 'Reinventing Data Protection?' (Springer, 2009).

self-determined, self-authored or self-created, following plans and ideals – a conception of the good – that they have chosen for themselves."[50]

De Hert and Gutwirth[51] note that, on a general level, the European Convention on Human Rights (ECHR) fails to cater for the rights to autonomy and individual self-determination. They argue that this approach is "*not unwise*", particularly in light of the constitutional differences among Member States[52]. For instance, German case law developed the principle of informational self-determination in regard to personal data based on the German constitutional concept of self-determination[53]. On the other hand, the Dutch and Belgian constitutions consider data protection as emerging from the right to privacy[54].

Notwithstanding this, case law of the European Court of Human Rights (ECtHR) has indicated that Article 8 ECHR (right to private life) confers a degree of protection over personal autonomy. In *Pretty v. The United Kingdom*[55] the ECtHR held that "*though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees*."[56] Moreover, in their joint dissenting opinion, to *Odievre v. France*[57], judges Wildhaber, Bratza, Bonello, Loucaides, Cabral Baretto, Tulkensand Pellonpaa

[50] Ibid 60.
[51] P. De Hert and S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (eds.) 'Reinventing Data Protection?' (Springer, 2009).
[52] Ibid 14.
[53] Ibid.
[54] Ibid.
[55] Ibid (n 2).
[56] Ibid (n 2).
[57] *Odievre v France*, App. No. 42326/98 (ECtHR, 13th February 2003).

held as follows: "*we are firmly of the opinion that the right to an identity, which is an essential condition of the right to autonomy is within the inner core of the right to respect for one's private life.*"[58]

One of the central notions of this thesis, together with the concept of big data and data protection, is the value of personal autonomy. As seen above, while there exists no specific or express right to personal autonomy or individual self-determination, this value seems to stem from the fundamental right to private life. Data protection, in seeking to safeguard the right to private life, also works so as to protect the value of personal autonomy and the individuals' right to "shape their own future through voluntary action". It confers such protection by regulating the manner in which personal data is processed and managed by data controllers. It is important to note here that we are speaking of the right to personal autonomy of living individuals – naturally, the deceased can hardly "shape their own future through voluntary action" once they have passed away.

3. BIG DATA – THE NEW THREAT TO PERSONAL AUTONOMY

3.1 What is "Big Data"?

Present literature provides an array of definitions of the term "big data"; however for the purposes of this thesis, the author has chosen the definition provided by the Article 29 Data Protection Working Party:

[58] Dissenting opinion of Judges Wildhaber, Bratza, Bonello, Loucaides, Cabral Baretto, Tulkensand Pellonpaa to the judgment delivered in the case *Odievre v France* (see Ibid).

"Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals."[59]

3.2 The Risks of Big Data

3.2.1 Data Protection Concerns

A large part of the concerns that the advent of big data in general has brought with it are related to privacy and data protection. In 2012, the UN Global Pulse noted that "*the wealth of individual-level information that Google, Facebook, and a few mobile phone and credit card companies would jointly hold if they ever were to pool their information is in itself concerning. Because privacy is a pillar of democracy, we must remain alert to the possibility that it might be compromised by the rise of new technologies, and put in place all necessary safeguards."*[60] This fear was recently echoed by the European Data Protection Supervisor who writes: "*these growing markets pose specific risks to consumer welfare and to the rights to privacy and data protection.*"[61] The European Parliament has also voiced its apprehensions, calling on businesses providing new

[59] Article 29 Data Protection Working Party 00569/13/EN WP 203, Opinion 03/2013 on purpose limitation adopted on 2 April 2013.
[60] UN Global Pulse, Big Data for Development: Challenges & Opportunities, May 2012 accessed via http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf on 28th June 2014.
[61] Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014 accessed via https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf on 28th June 2014.

services using big data to build in data protection measures already at the development stage, in order to maintain a high level of trust among citizens[62].

3.2.2 From Correlations to Predictions – The Threat to Personal Autonomy

In addition to the risks associated with data processing in general, big data has brought its own concerns. Particularly, big data analytics are leading to the discovery of connections between data, generating predictions of future events on the basis of correlation rather than causation[63]. Perhaps the most-mentioned prediction in big data literature is the Google Flu Prediction[64]. Google claimed to be able to detect influenza epidemics using search engine query data. Medical experts compared the data from Google Flu Trends between 2003 and 2008 and found that the predictions were rather accurate as regards illnesses such as colds that seemed like the flu, but they did not predict the actual flu very well. The mismatch was due to the presence of infections causing symptoms that resemble those of influenza, and the fact that influenza is not always associated with influenza-like symptoms[65]. Notwithstanding this, the fact that Google could identify, even if perhaps with not absolute accuracy, trends relating to the flu by means of data generated from search queries is still rather impressive.

---

[62] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20140312+ITEMS+DOC+XML+V0//EN&language=EN#top on 28th June 2014.

[63] M. Hilderbrandt, *Slaves to Big Data. Or Are We?* (Selected Works of Mireille Hildebrandt) accessed via http://works.bepress.com/mireille_hildebrandt/52 on 28th June 2014.

[64] See http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en/us/archive/papers/detecting-influenza-epidemics.pdf and http://www.google.org/flutrends/ accessed on 28th June 2014. Also see UN Global Pulse, *Big Data for Development: Challenges & Opportunities*, May 2012 accessed via http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf on 28th June 2014.

[65] See Ibid (n 60).

Big data predictions are bound to have an impact on the daily lives of individuals for future generations to come[66]. Moerel[67] describes this phenomenon as "*looking for the 'what', without knowing the 'why'*"[68]. Governments and private entities may act on these correlation-based predictions, for instance to determine insurance rates, to decide on whether to award or deny loans, or perhaps even to prevent crimes[69]. Big data analytics may therefore yield predictions about individuals which may preclude their freedom of choice and threaten their personal autonomy[70]. Individuals are at risk of being told who they are and what they like[71]. In this regard, Mayer-Schonberger and Cukier[72] argue that the promise of big data is to generate the same results as profiling does, only with less discrimination and more individualization[73]. They argue that:

> *"If big data predictions were perfect, if algorithms could foresee our future with flawless clarity, we would no longer have a choice to act in the future. We would behave exactly as predicted. Were perfect predications possible, they would deny human volition, our ability to live our lives freely."*[74]

[66] See B. Marr, *Big Data: The Mega-Trend That Will Impact All Our Lives*, 27th August 2013 accessed via https://www.linkedin.com/today/post/article/20130827231108-64875646-big-data-the-mega-trend-that-will-impact-all-our-lives on 29th June 2014; and R. Hutchins, *Perspective: Looking Forward to Life with Big Data*, 2nd January 2014 accessed via http://emcien.com/perspective-looking-forward-life-big-data/ on 29th June 2014.
[67] Ibid (n 26).
[68] Ibid (n 26) 8.
[69] V. Mayer-Schonberger and K. Cukier, *Big Data: A Revolution that will Transform How We Live, Work, and Think* (First Mariner Books, 2014).
[70] Centre for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance* (Discussion Document, Hunton & Williams LLP, February 2013) 2.
[71] Ibid (n 26) 41.
[72] Ibid (n 69).
[73] Ibid (n 69) 161.
[74] Ibid (n 69) 161.

While perfect predictions may still be far off in our future, big data analytics can already deliver probable predictions[75]. On this point, Richards and King[76] argue that big data has three paradoxes, one of which is the identity paradox – "*big data seeks to identify, but it also threatens identity*"[77]. They argue that the right to identity emanates from the right of individuals to make free choices about who they are and that big data threatens the personal autonomy of individuals. This issue is summed up perfectly by Leonard[78] who argues that:

> *"The companies that figure out how to generate intelligence from that data will know more about us than we know ourselves, and will be able to craft techniques that push us toward where they want us to go, rather than where we would go by ourselves if left to our own devices*."[79]

Hildebrandt[80] explains the situation by referring to the claims made by some advocates of big data that in big data analytics, the sample chosen for analysis equals the entire population. She argues that "*if it were true big data could rupture any membrane that shields our inner lives, disrupting the most sacred place of both privacy and autonomy, because it would allow its masters to know us better – and to know anything better – than we do ourselves. If it were untrue, big data could still uproot our sense of self and our interface with the world, to the extent that we cannot contest*

[75] For instance, a professor in the University of Pennsylvania claims that, using big data analytics, he can predict the probability that a parolee will be involved in a homicide when released. See Ibid (n 250) 161 – 162 for more details.
[76] N. M. Richards and J. H. King, *Three Paradoxes of Big Data* (Stanford Law Review Vol. 66:41, 2013).
[77] Ibid 43.
[78] A. Leonard, *How Netflix is Turning Viewers into Puppets* (Salon, 1st February 2013).
[79] Ibid.
[80] Ibid (n 63).

its outcomes, we have trouble to resist the seemingly clean, objective knowledge it produces and we do not have the tools to figure out how we are being profiled."[81]

Notwithstanding all of the above, one must keep in mind that once an individual passes away, there remains no future to shape. Any decisions an individual would want to have the liberty of making would only be possible during his lifetime. The value of personal autonomy is of no significance to an individual after death. In light of this, the risks which the advent of big data analytics brings to the fore of personal autonomy can hardly be said to be of concern to deceased persons. It is indeed the living individuals who are at risk of being deprived of their personal autonomy and it is this very risk that makes it onto the agenda of the data protection regime. Through data protection, living individuals' value of personal autonomy and self-determination (among other values) is sought to be safeguarded.

[81] Ibid (n 48) 2.

Chapter II

Is Data of Deceased Persons Used In Big Data Analytics?

1. SCOPE AND PURPOSE

Technological developments have led to increased storage capacity at relatively low costs, bringing about a widely-adopted attitude of "forgetting-by-selection" and "remembering-by-default" instead of the other way around[82]. This chapter shall revolve around this apparent longevity of data and focus on the place of data of deceased individuals in big data analytics. Specifically, the author shall examine whether data controllers involved in big data analytics distinguish between data pertaining to living and deceased individuals when attempting to identify trends. The assessment to be carried out shall be restricted to data controllers in the private sector. The author has chosen to study the policies and practices of seven private companies selected from different environments in the online market so as to adopt a multi-faceted approach. Each of the companies are involved in big data analytics and feature prominently in the online world.

The assessment shall be conducted in respect of:

- Google as a provider of a variety of essential online services including search engine services, email services and cloud services;
- Facebook as a social network provider;
- Spotify as an online music service provider;
- Amazon as an online retailer;
- eBay as an online platform for retailers and consumers;
- Ryanair as a commercial business providing its services online; and

[82] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009). Also see presentation delivered by P. Korenhof, 'Timing the Right to be Forgotten', delivered at the Computers, Privacy and Data Protection Conference on 23rd January 2014 accessed via http://www.cpdpconferences.org/Resources/23_GH_1030_KORENHOF.pdf on 16th June 2014.

- Zynga as an online game service provider.

2. GOOGLE

Google Trends, "*a real-time daily and weekly index of the volume of queries that users enter into Google*"[83], has been collecting information since 2004 for the purpose of identifying trends from search engine queries inputted by Google users[84]. A recent example of trend identifications undertaken by Google is that carried out in respect of the 2014 World Cup[85]. Through an analysis of search queries entered in relation to the final game between Germany and Argentina, Google identified German supporters as feeling "unstoppable", whereas Argentinian supporters were held to be feeling "proud"[86].

The Google Cloud Platform was also struck by the World Cup fever, issuing predictions of game wins and getting it right 13 out of 14 times prior to the final games for which a "*narrow win*" was predicted for Germany[87]. To sum it up, Google predicted the winner of the 2014 World Cup finals (among several other games) based on analysis conducted in respect of "*data from Opta covering multiple seasons of professional soccer leagues as well as the group stage of the World Cup*" combined with *"a power ranking of relative team strength developed by one of our engineers, as well as a metric stand in for home team advantage based on fan enthusiasm and the number of*

[83] H. Choi and H. Varian, *Predicting the Present with Google Trends* (The Economic Record, Vol. 88, Special Issue June 2012) 2 – 9.
[84] See Google Trends accessible via http://www.google.com/trends/.
[85] See http://www.google.com.mt/trends/worldcup#/en-us/ accessed on 20th July 2014.
[86] See http://www.google.com.mt/trends/worldcup#/en-us/match/64/ accessed on 20th July 2014.
[87] See http://googleblog.blogspot.com/2014/07/google-cloud-platform-predicts-world.html accessed on 20th July 2014.

fans who had travelled to Brazil"[88]. Data generated from Google searches carried out by its users has proven to yield other predictions, for instance in the case of prediction of housing prices and sales[89] and flu trends[90].

In generating information Google collects personal information, such as the name, email address, telephone number or credit card, from its users for the purposes of creating a Google Account. Users may even set up a Google Profile which may include a photograph of the user. In addition to information provided by the user, Google also collects information about the user from the latter's use of Google's services. For instance, Google collects information about which services the user makes use of, for what purpose and in which manner he uses them, how frequently he uses them etc. Google also collects information about how users view and interact with adverts and content provided by Google[91].

Information collected by Google in this regard includes device-specific information (such as unique device identifiers); log information (for instance, telephony log information like the time, date and duration of calls); location information; local storage (such as browser web storage); and cookies and anonymous identifiers[92]. Google uses the information it collects from and about its users to offer tailored content to them, mainly by providing more search results and advertisements to suit the needs of each individual user[93].

---

[88] Ibid.
[89] L. Wu and E. Brynjolffson, *The Future of Prediction: How Google Searches Foreshadow Housing Prices and Sales*, draft of May 2014 accessed via http://www.nber.org/chapters/c12994.pdf on 21st July 2014.
[90] Ibid (n 60).
[91] Google Privacy Policy, accessed via https://www.google.com.mt/policies/privacy/#infouse on 18th July 2014.
[92] Ibid.
[93] Ibid.

Google has opted to take on a rather proactive approach towards the handling of data pertaining to deceased users by setting up an Inactive Account Manager feature. This feature is intended to allow the user to pre-determine what happens to his account, and who can access it, following his death. The purpose of the Inactive Account Manager is primarily to provide a way for users to share their data (in part or in whole), or to notify a third party if they have been inactive for a specified period of time. Inactivity of a user's account is detected through the recording of usage pattern data by Google as are sign-ins, web history and account usage[94].

A user can choose to have his account deleted, the effects of which will vary according to the products which are subscribed to through that account. Upon deletion, an account will no longer be accessible and the same username cannot be reused thereafter. The user may also opt to appoint a trusted contact who will be able to receive access from Google to download the user's data[95]. Upon detecting inactivity, Google will warn the user by sending a text message on the mobile phone number provided by the user and by sending an email to a secondary email address also provided by the user[96].

In the event that a deceased user would not have set up an Inactive Account Manager, Google does not automatically provide access to his account to survivors. In particular, Google's policies make it very clear that Google may, but is not obliged to, provide access to an authorised representative of the deceased, only in rare cases[97]. The requestor is required to provide certain information about

[94] Google Help Page, *About Inactive Account Manager*. Accessed via https://support.google.com/accounts/answer/3036546?hl=en on 2nd February 2014.
[95] Ibid.
[96] Google Public Policy Blog, *Plan your digital afterlife with Inactive Account Manager*. Accessed via http://googlepublicpolicy.blogspot.nl/2013/04/plan-your-digital-afterlife-with.html on 3rd February 2014.
[97] Gmail Account Access Issues, *Accessing a deceased user's mail*. Accessed via https://support.google.com/mail/answer/14300?hl=en on 3rd February 2014.

himself[98], information to verify a connection between the requestor and the deceased user[99] and a death certificate of the deceased. Upon receiving these documents, Google will assess the application and determine whether the request is eligible to move on to the second phase of the process. No indication of the criteria upon which this decision is to be made is given to the requestor however. Should the application move on to the second phase, the requestor will be required to provide an order from a US court and/or additional materials. There is however no upfront specification of what these additional materials may consist of. Google further retains the right not to disclose the reasons for its decision should it determine that request shall not be acceded to[100].

In 2010 an interview[101] with Google's privacy personnel shed light on its data retention practices. Whitten, a security and privacy engineer at Google, explained that Google aims to keep retention periods to a minimum, while extracting the maximum value from the data possible within that time frame. Data was argued to be needed to "*learn from the good guys, fight off the bad guys,* [and] *invent the future*"[102]. Four years later Google's privacy policy, last updated on 31st March 2014, states that "*we aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information*

[98] Including full name, physical mailing address, email address, government-issued ID or driver's license.
[99] Namely the deceased user's email address and specified content from an email sent from that account to the requestor's account.
[100] Ibid (n 97).
[101] See N. Anderson, *Why Google Keeps Your Data Forever, Tracks You with Ads*, 8th March 2010, accessed via http://arstechnica.com/tech-policy/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys/ on 18th July 2014.
[102] Ibid.

from our backup systems"[103]. This seems to imply that even when users delete their data, Google will retain a copy on its backup systems indefinitely.

3. FACEBOOK

It is an undisputed fact that Facebook harbours a gold mine in terms of data, considering that its users "*send 10 billion Facebook messages per day, click the 'like' button 4.5 billion times and upload 350 million new pictures each and every day. Overall, there are 17 billion location-tagged posts and a staggering 250 billion photos on Facebook.*"[104] Marr[105] believes that "*if we all stopped using Facebook today, the company would have enough detailed insights about us to exploit that for years. No other company in history has ever possessed this level of detailed personal information and I believe that, apart from Google maybe, there is no other company on the planet that comes close to those levels of 'intemate' big data.*"[106]

Facebook collects certain personal information about its users for the purposes of registration, such as name, email address, birthday and gender. Information users choose to share, which can range from status updates and comments to "liking" pages and adding friends, is also gathered by Facebook. Information provided by one user about another user, for example through the use of tagging and invites, also makes the list of data collected by Facebook. In addition to this, Facebook stores information about user activity, such as when users look at other users' timelines, receive

[103] Ibid (n 91).
[104] B. Marr, *Facebook's Big Data: Equal Parts Exciting and Terrifying?*, 18th February 2014 accessed via http://smartdatacollective.com/bernardmarr/185086/facebook-s-big-data-equal-parts-exciting-and-terrifying on 23rd July 2014.
[105] Ibid.
[106] Ibid.

messages, use a Facebook mobile app, make purchases through Facebook and the like[107]. The data collected by Facebook is then used to offer and suggest services and features. Facebook gets to know its users through the information it collects about them in order to make friend suggestions, suggest people to tag in photos, inform the user of friends who are in a nearby location as the user, offer deals which might interest the user etc[108].When a user deletes information which he previously made available on Facebook, for instance a status update, Facebook will remove it from the website. Some of this information will be permanently deleted from Facebook's servers; however parts of this information will remain stored by Facebook until the user permanently deletes his account. The reason for this retention is for Facebook to be able to provide its users with a better user experience, for instance by not suggesting friends from whom the user would have rejected friend requests[109].

In the event that a Facebook user wishes to cease making use of Facebook's services, he may choose from two options: deactivating or deleting his account[110]. In the former case, none of the information attached to the user account is deleted, allowing the user to reactivate the account at a later stage. In the latter case, Facebook's data use policy explains that "*it typically takes about one month to delete an account but some information may remain in backup copies and logs for up to 90 days…Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message…That information remains after you delete your account.*"[111]

[107] Facebook Data Use Policy accessed via https://www.facebook.com/about/privacy/your-info on 18th July 2014.
[108] Ibid.
[109] Facebook FAQs, *What happens to content (posts, pictures) that I delete from Facebook?*, accessed via https://www.facebook.com/help/356107851084108 on 18th July 2014.
[110] Ibid (n 107).
[111] Ibid (n 107).

As regards deceased users, initially Facebook dealt with the death of a user by removing the account, rendering the timeline of the user and all associated content inaccessible to other Facebook users[112]. Eventually a "memorialization feature" was introduced, retaining the user's timeline but removing some functionalities from the account. Accounts are memorialized upon request by survivors of the deceased – proof of death must be provided; however there is no need for the requestor to have a specific relationship with the deceased[113]. A request may also be made for the removal of an account of a deceased user; however this possibility is restricted to immediate family members upon presenting proof of death and proof that they are the lawful representatives of the deceased and the relative estate[114]. Therefore it seems that information held in accounts which are memorialized is retained by Facebook after the user's death and only selected pieces of that information is deleted if the account is removed following the user's death.

Facebook also collects information about individuals who do not hold a Facebook account[115]. Facebook Connect, a system used to issue cookies, is included in a number of websites which can be visited by non-Facebook users. Upon visiting at least one of these websites, a cookie is placed on the individual's device and from that moment on, any browsing of websites which include the Facebook "like" button result in a request for the "like" button from the Facebook server including the cookie[116]. According to Roosendaal, the likelihood of coming across a website which has

[112] D. McCallig, *Facebook after death: an evolving policy in a social network* (International Journal of Law and Information Technology, Oxford University Press 2013) 1–34.
[113] Facebook Application Forms, *Special Request for Deceased Person's Account*. Accessed via https://www.facebook.com/help/contact/228813257197480 on 2nd February 2014.
[114] Facebook FAQs, *How do I submit a special request for a deceased user's account on the site?* Accessed via https://www.facebook.com/help/www/265593773453448 on 2nd February 2014.
[115] A. Roosendaal, 'We are All Connected to Facebook,…by Facebook!' in S. Gutwirth et al. (eds.), 'European Data Protection: In Good Health?' (Springer, 2012) 3 – 19.
[116] Ibid.

implemented Facebook Connect is rather substantial. The number of implementations was at approximately one million in March 2009, just one year after the introduction of Facebook Connect, and is exponentially increasing[117]. The manner in which Facebook uses this information, and when, if ever, it deletes data about non-users is unknown.

4. SPOTIFY

Spotify is without a doubt a data-driven company. "*Spotify users create 600 Gigabyte of data per day and 150 Gigabyte of data per day via different services. Every day 4 Terabyte of data is generated in Hadoop, a 700-node cluster running over 2,000 jobs per day. They currently have 28 Petabytes of storage, spread out over 4 data centres across the world.*"[118]

Users are requested to provide personal information including their email address, date of birth, gender, postal code and country in order to register an account with Spotify. Any information which users may voluntarily add on to their profile, such as a telephone number, will also be stored by Spotify[119]. Other information collected by Spotify includes data inferred from user activity, for instance, information about the type of subscription, the user's interactions with and use of the service, technical data such as the user's IP address and location information[120]. Users are able to connect to Spotify through their Facebook account, in which case data available on the user's Facebook profile is automatically collected by Spotify. This data includes the username, encrypted

[117] Ibid (n 115).
[118] *How Big Data Enabled Spotify to Change the Music Industry* accessed via http://www.bigdata-startups.com/BigData-startup/big-data-enabled-spotify-change-music-industry/ on 19th July 2014.
[119] Spotify Privacy Policy accessed via https://www.spotify.com/uk/legal/privacy-policy/#information on 18th July 2014.
[120] Ibid.

access credentials, name, profile picture, country, email address, date of birth, gender, friends' names and profile pictures and networks[121].

The information collected by Spotify is mainly used to improve user experience when making use of Spotify services, to ensure technical functioning of the service and develop new products and to communicate promotional material regarding the services to the user[122]. Users who choose to connect to Spotify using Facebook will automatically have data relating to their activity shared with Facebook. Spotify may also share information collected about its users, such as musical preferences, settings and technical data, with providers of third party applications. However, it claims that precautions are taken to prohibit third party application providers from attempting to identify users through the information provided to them or by collecting additional information without user consent[123].

Spotify's privacy policy does not provide any information on the duration for which data is retained by Spotify. No information is provided on whether data attached to a user account is deleted from Spotify's servers at any point in time, for instance upon deletion of the account. Moreover, there is no mention of what happens to data held in a user account once the user passes away either.

[121] Ibid.
[122] Ibid.
[123] Ibid.

5. AMAZON

Amazon[124] collects most of the data about its users when they search, buy and post items, participate in a contest or questionnaire or communicate with customer service. Information generally provided to Amazon by users includes name, address, telephone number, credit card information, information about people to whom purchases have been dispatched, contents of reviews and emails sent to Amazon, the personal description and profile picture included in the user's profile and financial information[125]. In addition to this, Amazon also collects and analyses certain automatic information, including the user's IP address, login credentials, computer and connection information, purchase history, cookie number and products viewed or searched for[126].

Amazon's main scope for collecting data about its users is to personalise and continually improve their shopping experience on its website. Information is used to handle orders, deliver items, process payments, communicate with users regarding their orders and promotional offers, provide content such as customer reviews to users and recommend items that might be of interest to users. Amazon also uses cookies in order to enable its systems to recognize a user's device and provide features to users[127]. In certain instances, Amazon shares information collected about its users with third parties, such as affiliated businesses and third party service providers[128].

[124] This assessment has been conducted in respect of Amazon.co.uk.
[125] Amazon.co.uk Privacy Notice accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=gss?nodeId=502584 on 19th July 2014.
[126] Ibid.
[127] Ibid.
[128] Ibid.

Amazon has been reported to use "*big data to monitor, track and secure its 1.5 billion items in its retail store that are laying around its 200 fulfilment centres around the world. Amazon stores the product catalogue data in S3. This is a simple web service interface that can be used to store any amount of data, at any time, from anywhere on the web. It can write, read and delete objects up to 5 TB of data each. The catalogue stored in S3 receives more than 50 million updates a week and every 30 minutes all data received is crunched and reported back to the different warehouses and the website*."[129]

There is no reference to data retention periods adopted by Amazon, or any indication of when, if at all, user data is deleted from their servers. However, some thorough browsing of Amazon's website reveals sporadic instances where users are enabled to manage certain information which Amazon collects about them. In particular, users are allowed to add or update information contained in their account (but no mention of whether data can be deleted by users is made)[130] but Amazon will still keep a copy of older versions of user information[131]. Users are also able to delete their Amazon browsing history[132]. As regards the death of Amazon users, neither the privacy notice nor Amazon's terms and conditions[133] seem to cater for this scenario. Furthermore, it seems that closing or deleting an Amazon user account is no easy feat[134], rendering it not only difficult

[129] *How Amazon is Leveraging Big Data* accessed via http://www.bigdata-startups.com/BigData-startup/amazon-leveraging-big-data/ on 19th July 2014.

[130] See Amazon Help Page, *Edit Your Profile*, accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=help_search_1-7?ie=UTF8&nodeId=200039420&qid=1405938238&sr=1-7 on 20th July 2014.

[131] Ibid (n 80).

[132] See Amazon Help Page, *Manage Your Browsing History* accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=help_search_1-1?ie=UTF8&nodeId=15891461&qid=1405938359&sr=1-1 on 20th July 2014.

[133] Conditions of Use and Sale accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=1040616 on 20th July 2014.

[134] See R. Hopkins, *The Day I Closed My Amazon Account*, 5th December 2013 accessed via https://www.transitionnetwork.org/blogs/rob-hopkins/2013-12/day-i-closed-my-amazon-account on 20th July 2014.

to close one's own account, but much more so when the account belongs to a deceased individual. Even if a deceased user's account is somehow closed, there does not seem to be anything in Amazon's policies to indicate that the user's information will be deleted from Amazon's servers once the account is closed.

6. EBAY

During the Gartner CRM Summit in London, David Stephenson, head of global business analytics at eBay, explained that the company's aim is for eBay to apply big data analytics in such a manner that it will be able to offer the same kind of personalization as one would expect from a small shop[135]. "*In monitoring their 100 million customers' interactions - from every button they click to every product they buy - eBay creates 12TB of data per day which is continually added to a 4 petabyte table containing 4tn rows of data. As the data is queried both by automatic monitoring systems and employees looking to find more meaning from it, data throughput reaches 100 petabytes (102,400TB) per day.*"[136]

In order to register an account with eBay[137] users need to provide certain information, including email address, phone number, physical contact information and financial information. Users may also supply eBay with information about them through other means, for instance via social media websites or services, by requesting transactional information for the purpose of providing a service,

[135] C. Saran, *Case Study: How Big Data Powers the EBay Customer Journey*, 29th April 2014 accessed via http://www.computerweekly.com/news/2240219736/Case-Study-How-big-data-powers-the-eBay-customer-journey on 20th July 2014.
[136] M. Passingham, *eBay Using Big Data Analytics to Drive Up Price Listings*, 22nd October 2013 accessed via http://www.v3.co.uk/v3-uk/news/2302017/ebay-using-big-data-analytics-to-drive-up-price-listings on 20th July 2014.
[137] This assessment has been carried out in respect of eBay.co.uk.

or through their activity and use of the eBay website. eBay may also ask users to provide additional information about themselves, such as a copy of an identification document or a bill, in order to verify the user's address or verify his identity[138].

Additional information may be collected by eBay through mobile applications, such as geo-location information, and from other third party sources, such as demographic and navigation information and credit check information[139]. eBay offer services which enable users to share information with third party social media websites, such as Facebook and Twitter. Users may choose to allow eBay to access information about them held by these third party websites. By giving access to eBay, users allow it to collect, use and store information from these websites in accordance with eBay's privacy policy[140].

In addition to functional purposes, eBay uses the information it collects about its users to customize, measure and improve its services, content and advertising and to deliver targeted marketing and promotional offers. eBay also informs its users that it may combine their personal information with information collected from other sources for the purposes of offering personalized advertising and marketing to them[141].

eBay users are able to access, review and change most of their personal information and eBay assures users that it will honour any statutory right that a user may have to erase or modify his

[138] eBay Privacy Notice accessed via http://pages.ebay.co.uk/help/policies/privacy-policy.html?rt=nc on 20th July 2014.
[139] Ibid.
[140] Ibid.
[141] Ibid.

personal information[142]. When a user closes his eBay account, eBay's privacy policy confirms that the personal information held therein will be removed so that it cannot be viewed by other users. eBay reserves the right to cancel or deactivate accounts which are "*inactive for a long time*", without specifying what period of time can be considered "*a long time*". Information held in closed or inactive accounts will be deleted or rendered anonymous by eBay as soon as is reasonably possible after closure or deactivation of the account. However, under certain circumstances, such as for the purposes of fraud prevention or collection of fees owed, eBay may retain personal information from closed or inactive accounts for longer[143].

While eBay's privacy policy does not specifically mention what happens to users' accounts and the personal information held therein upon their death, the actions it takes in respect of inactive accounts seem to be a step towards catering for this scenario. The lack of a clarification as to what can be considered "*a long time*" however tends to blur the lines, leaving room for an account to remain open for a period of time following the death of the user, during which eBay may process the data pertaining to him.

7. RYANAIR

Ryanair is not a stranger to big data analytics either, with its CEO, Michael O'Leary, announcing that "*we'll build individual profiles for each passenger. We'll know how often you fly, where you*

[142] Ibid.
[143] Ibid.

fly, who you fly with and we'll design individual packages for you."[144] Ryanair have even entered into a partnership with Google and "*while both Google and Ryanair are tight-lipped about what exactly the partnership will entail, at the heart of the deal is bound to be so-called "Big Data".*"[145] Google has set up a dedicated flight search capability which provides users with an easy method of comparing prices offered by different airlines[146]. When a user selects a Ryanair flight, he is directed to Ryanair's booking page for that specific flight. Ryanair has confirmed that it will not be investing any money into this deal, but will rather be sharing its data with Google[147].

Among the personal data collected by Ryanair from its users are passenger names, addresses, passport or identity card numbers, telephone numbers, email addresses and IP addresses and payment details. In certain cases Ryanair also collects certain medical information from its users in the event that the user suffers from a medical condition which may affect the flight arrangements[148]. Some of the purposes for which information is used by Ryanair listed in its privacy policy are rather open and vague. For instance, purposes financial data verification or screening, immigration or customs control safety, security, health, administrative, crime prevention or detection, legal purposes, statistical and marketing analysis and systems testing[149]. Ryanair also uses tracking software and cookies to monitor customer traffic patterns and activity on its website for the purposes of improving the design and layout of the websites[150].

---

[144] *Ryanair and Google Set Out to Disrupt Travel Distribution*, 14th January 2014 accessed via http://thinkdigital.travel/knowledgestream/ryanair-and-google-set-out-to-disrupt-travel-distribution/ on 20th July 2014.
[145] E. O' Loughlin, *The Ryanair and Google Partnership – What's In It For Us?*, 31st January 2014 accessed via http://businessetc.thejournal.ie/readme/ryanair-and-google-partnership-%E2%80%93-what%E2%80%99s-in-it-for-us-1291150-Jan2014/ on 20th July 2014.
[146] See https://www.google.com/flights/ accessed on 20th July 2014.
[147] Ibid (n 145).
[148] Ryanair Website Privacy Statement accessed via http://www.ryanair.com/mt/privacy-policy/ on 20th July 2014.
[149] Ibid.
[150] Ibid.

Users of the Ryanair website are also able to register an account with Ryanair in order to have their booking details saved and entered automatically when making future bookings[151]. Information collected for registration purposes includes the user's name, email address, telephone number, billing details and payment details[152]. Any data about users collected by Ryanair can be disclosed to third party service providers such as hotel, car hire and credit card providers upon the consent of the user. It is not clear whether the sharing of data with Google in light of their partnership is covered under this statement of the privacy policy. This may potentially mean that Google processes this data in accordance with its own policies.

As regards data retention practices, Ryanair's privacy policy does not provide any information on the retention periods adopted by it or whether data which it collects about its users is ever deleted. No mention of the death of a user and how a deceased user's information is managed is made either.

8. ZYNGA

"*On a regular day Zynga delivers one petabyte of content. In order to cope with these extreme high demands of data, they have built a flexible cloud server centre that can easily add up to 1.000 servers in just 24-hours. In fact, Zynga's private and public cloud server park is known as one of*

[151] See https://www.bookryanair.com/SkySales/Booking.aspx?culture=en-ie&lc=en-mt#Register accessed on 20th July 2014.
[152] Ibid.

the biggest hybrid clouds."[153] Zynga games are offered to users through social network sites such as Facebook and Google+. When users play Zynga games through these sites, Zynga gains access to certain information about the user held in his social network profile, subject to the privacy settings selected by the user on the social network site[154]. Information which may be accessed by Zynga in such cases includes name, profile picture, user ID number, user ID numbers and other public information of friends of the user, email address used for logging in to the social network site, physical location, gender and birthday[155]. This information may also be provided to Zynga when a user sets up an account with Zynga using Facebook Connect or other social network site authentication options[156].

Zynga enables users to import their address book contacts or to manually enter email addresses for the purposes of locating contacts on Zynga and inviting other users to join in Zynga games[157]. Therefore a person's email address can be stored by Zynga without any action being taken by him. Billing and financial information is collected from users who purchase a license to use in-game virtual currency or virtual items directly from Zynga or through third parties such as Facebook or Apple[158]. Zynga also collect certain technical information about users' devices and usage statistics about users' interactions with the service. Users who download the Zynga branded toolbar are also given the option to provide certain personal information, for instance through its contact form[159]. Additionally, Zynga records and stores archives of communications carried out by users through

[153] *Zynga is a Big Data Company Masqueraded as a Gaming Company* accessed via http://www.bigdata-startups.com/BigData-startup/zynga-is-a-big-data-company-masqueraded-as-a-gaming-company/ on 20th July 2014.
[154] Zynga Privacy Policy accessed via https://company.zynga.com/privacy/policy on 20th July 2014.
[155] Ibid.
[156] Ibid.
[157] Ibid.
[158] Ibid.
[159] Ibid.

participation in player forums and message boards, posting public comments to other users' profiles or gameboards, sending private messages or invitations to other users, chatting with other users and posting photos[160].

Zynga uses cookies to collect certain technical information about its users for the purposes of analysing the usage of its websites and services, to provide a more personalized experience for users and to manage advertising. Zynga also collects information from other sources, including third party information providers, which it uses to supplement the information gathered about a user[161]. Among other purposes, Zynga uses the information it collects for game and service functionality reasons, to enable user-to-user communications, to deliver and target advertising and to solicit input and feedback to improve Zynga products and services and customize user experience[162]. Zynga shares user information (including personal information in some cases) with third party service providers, friends of the user and other Zynga players and third party advertisers. In the latter case, information is aggregated or anonymous and does not specifically identify a user[163].

Zynga offers users the option to access and update their information and to manage their privacy settings. Users who do not wish Zynga to make active use of their information may contact Zynga to delete their account. Certain information will however be kept by Zynga even post-deletion for legal and accounting purposes. Content posted on the service by users may also not be possible to

[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Ibid.

delete[164]. Zynga's privacy policy does not reveal any data retention periods applied by Zynga and it has been claimed that Zynga's database keeps growing because it never deletes any data due to the complex process that deletion requires[165]. Therefore it would seem that unless action is taken by a user, his data will continue to be stored and processed by Zynga indefinitely. Zynga's privacy policy even explains that a game or other account with Zynga will be considered to be active unless a user files a request for its deletion or deactivation[166]. In the case of a deceased user, it appears that Zynga will continue to consider his account to be active indefinitely.

9. OBSERVATIONS

While the exercise conducted above can far from provide an absolute account of practices adopted by all entities performing big data analytics following the death of their users, it still serves to shed some light on the matter. One particularly noteworthy observation is that none of the data controllers assessed seem to adopt any specific data retention periods. It appears that data is stored by these companies on an indefinite basis unless a specific request for deletion is made by users or their survivors, if this is even made possible at all. Moreover, even when a request for deletion is possible, some companies still retain some of the data on their servers after executing the deletion request.

This observation is supported by Herold who explains, "*I've talked with many organizations about their big data use. I've read many studies and articles. I've not found any that indicate they will*

[164] Ibid.
[165] See Ibid (n 153).
[166] Ibid (n 154).

delete big data repositories. In fact, all have indicated that they instead typically view them as infinitely growing repositories; the bigger the better! As more data is collected and retained, the more easily analytics will be able to determine more insights into individuals' lives."[167] The mentality of "big data hoarding"[168], where it is believed that "*all information is nearly equal in value, and that the more information a business can save, the better chance they have at deriving value from it later*"[169] further encourages data controllers to collect as much data as possible and to retain it for as long as possible.

We have seen that Google and Facebook have opted to devise a policy which deals with the management of data once the data subject passes away. This approach has also been adopted by other data controllers not mentioned here, such as Twitter[170] and Dropbox[171]. However, the

[167] R. Herold, *10 Big Data Analytics Privacy Problems*, 30th June 2014 accessed via http://midsizeinsider.com/en-us/article/10-big-data-analytics-privacy-problems on 23rd July 2014.
[168] See S. Drew, *Big Data Hoarding can be a Big Problem*, 11th July 2014 accessed via http://midsizeinsider.com/en-us/article/big-data-hoarding-can-be-a-big-problem on 23rd July 2014; and J. Clark, *Big Data or Big Data Hoarding?*, 14th March 2013 accessed via http://www.datacenterjournal.com/it/big-data-big-data-hoarding/ on 23rd July 2014 for more information on the problems that 'big data hoarding' gives rise to.
[169] See S. Drew, *Big Data Hoarding can be a Big Problem*, 11th July 2014 accessed via http://midsizeinsider.com/en-us/article/big-data-hoarding-can-be-a-big-problem on 23rd July 2014.
[170] Twitter's deceased user policy was introduced in 2010, enabling the person acting on behalf of the deceased's estate or immediate family members to request the deactivation of the deceased user's account. A request for deactivation must be accompanied with documentation to verify the relationship of the requestor with the deceased as well as the death of the user. The proof required by Twitter includes the user's death certificate, a copy of the requestor's government-issued identity card and a statement from the requestor providing information and an official request for deactivation. It is unclear whether the data pertaining to the account will be retained by Twitter or deleted upon deactivation. However, the term "deactivation" in itself seems to indicate that the account will remain in existence, and will merely be inaccessible, hence implying that the data will be retained by Twitter. See Twitter FAQs, *Contacting Twitter about a Deceased User*. Accessed via https://support.twitter.com/articles/87894-contacting-twitter-about-a-deceased-user on 2nd February 2014 for more information.
[171] In the event of the death of a user, Dropbox's first approach is to suggest to survivors that they attempt to access the user's account through files available on the user's computer. This will however only work if the user would have synced his Dropbox account with his computer. Failing this, Dropbox offer the possibility to file a request for access, without guaranteeing that the request will be acceded to. As in the case of Facebook, Twitter and Google, Dropbox require that the requestor submits certain documentation to prove the death of the user and that the requestor is duly authorised to gain access to the deceased's files. Among the documentation required is a valid court order establishing that it was the deceased user's intent for the requestor to have access to the files following his death, and that Dropbox is compelled by law to provide these files to the requestor. There does not seem to be any time limit imposed by which requests for access need to be filed by survivors of the deceased, potentially implying that Dropbox will retain the

policies adopted deal with the account or profile of a user in general and not the actual data contained therein. Even in cases where a policy to cater for accounts or profiles after death is in place, data pertaining to deceased users seems to still be retained by the data controllers. The general approach towards dealing with data of deceased individuals seems to revolve mostly around matters of accessibility and closure of a person's account/profile after his death. Similarly to the perspective adopted in current literature on post-mortem data protection, the focus of these big data companies is on issues of control of user accounts, rather than on the actual harms which may ensue from the processing of data of deceased persons.

None of the big data companies examined above have given any indication of intending to remove data of deceased persons from their processing pool. Unless data controllers take specific action to distinguish data of deceased individuals from data of living individuals, how can the treatment allocated to these two sets of data differ? Furthermore, even if data controllers were to have a policy in place for the deletion or cessation of processing of data pertaining to deceased individuals, there exists another obstacle. How are data controllers to become aware of the death of a user? In instances where the user is able to set up a post-mortem plan for the use of his data, such as in the case of Google's Inactive Account Manager, action is still required on the part of the user. Unless the user is proactive and provides instructions to Google, the Inactive Account Manager has no function after his death. In most cases, such as with Facebook, data controllers depend on survivors of the deceased to inform them of his passing away. This gives rise to further complications; for instance, survivors of the deceased may not be aware of all the accounts held by the deceased. Moreover, in some cases survivors are required to provide a court order so as to

user's data indefinitely. See Dropbox Help Centre, *Can I access the Dropbox account of someone who has passed away?*, accessed via https://www.dropbox.com/help/488/en on 3rd February 2014 for more information.

be able to close the deceased's account with a company. This may be viewed as being too burdensome a task for the mere closing of an account, discouraging survivors from taking any action at all.

Finally, we have also seen that a number of data controllers tend to share their data with third parties, such as advertisers, rendering the data less within reach of its subject. In this regard Lessig[172] brings forth the example of websites synchronizing the cookies which they create. A person may provide his data to one company, and the website will then forward such data to other companies with which it is cooperating[173]. Naturally, the harder it is for a person to track his data, the harder it will be to notify the data controller of his death. In light of the above the author observes that, even if big data companies are willing to distinguish between data of deceased and living individuals, there exist certain obstacles on a practical level that render this difficult to achieve. Consequently, it appears that data, at least for the most part, tends to be retained by data controllers for purposes of big data analytics, even following the death of its subject.

[172] L. Lessig, *Code version 2.0* (Basic Books, 2006).
[173] Ibid 203.

Chapter III

Does Post-Mortem Data Protection Exist Within the European Union?

1. SCOPE AND PURPOSE

In this chapter the author seeks to establish whether a distinction is currently being made by data protection law in the EU on the basis of whether the data subject is living or deceased for the purposes of attributing protection thereto. There shall be three main areas of assessment:

- data protection as a human right under the Charter of Fundamental Rights of the European Union[174] and the European Convention of Human Rights[175];
- data protection under the Data Protection Directive and the proposed General Data Protection Regulation; and
- data protection in the national legislation of Member States of the EU.

2. DATA PROTECTION AS A HUMAN RIGHT

In their very essence, human rights are moral entitlements possessed by all human beings simply by virtue of their humanity[176]. Our eligibility to human rights distinguishes us from other organisms to the effect that to deny a person of these entitlements would be to deny him recognition as a human being. In this section, the author shall delve into two legal instruments which provide for a right to protection of personal data with the view of determining whether these are intended to benefit individuals even at a post-mortem stage. A brief overview of the general attitude adopted in the Charter of Fundamental Rights of the European Union and by the European Court of Human

[174] Charter of Fundamental Rights of the European Union (2000/C 364/01), 18th December 2000.
[175] Convention for the Protection of Human Rights and Fundamental Freedoms, 4th November 1950.
[176] J. Tasioulas, 'The Moral Reality of Human Rights' in Ethical and Human Rights Dimensions of Poverty: Towards a New Paradigm in the Fight against Poverty, Philosophy Seminar, UNESCO Poverty Project (All Souls College, Oxford, March 2003).

Rights towards applying human rights post-mortem shall be provided through an account of related case-law.

2.1 Charter of Fundamental Rights of the European Union

Article 8 of the Charter of Fundamental Rights of the European Union holds that:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority."*[177]

While the wording of this article in itself does not expressly indicate whether this right is afforded to both living and deceased individuals, consideration of the intention of the legislator helps to shed some light on the matter. In particular, when having a look at the second paragraph one will note that it sets the attainment of consent of a person to whom data relates as one of the means through which approval for the processing of data can be given. The same paragraph also grants the right of access and the right to rectification to the person to whom the data relates. The person these provisions refer to cannot possibly be deceased, as otherwise the second paragraph would

[177] Article 8 of the Charter of Fundamental Rights of the European Union, emphasis added.

make no logical sense. Therefore, while the wording itself does not preclude applicability of the right to deceased individuals, the spirit of the law points us in that direction.

2.2 European Convention on Human Rights

This section aims to examine if the European Convention on Human Rights (ECHR) provides protection of personal data once a data subject passes away. Section 2.2.1 will first consider if the ECHR system of rights contains a right to data protection. Section 2.2.2 will examine how the ECHR treats the issue of human rights protection of the deceased.

2.2.1 Does the ECHR System know a General Right to Data Protection?

The ECHR does not expressly cater for the right to data protection; however there exists case-law of the European Court of Human Rights (ECtHR) which interprets Article 8 of the ECHR, the right to protection of private life[178], as including data protection, albeit to a limited extent. For instance, in the case of *Leander v. Sweden*[179] the ECtHR held that "*it is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8(1).*"[180]

[178] Article 8 of the European Convention on Human Rights states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
[179] *Leander v. Sweden* App No 9248/81 (ECtHR, 26 March 1987).
[180] Ibid para. 48.

In the case of *Gaskin v. The United Kingdom*[181] the ECtHR concluded that confidential records concerning the applicant and his care as a foster child while he was a minor "*contained information concerning highly personal aspects of the applicant's childhood, development and history and thus could constitute his principal source of information about his past and formative years.*" [182] In light of this, the Court held that these records related to the applicant's private and family life in such a way that the question of his access thereto fell within the ambit of Article 8[183]. However, in reaching this decision the ECtHR expressly denied forming any opinion on whether general rights of access to personal data and information could be derived from Article 8. It explained that the Court was called upon to decide on the specific case of the applicant and not on questions of general principle[184].

The *Leander* case was quoted by the ECtHR in *Amann v. Switzerland*[185] where the Court held that the storing of data relating to the "private life" of an individual falls within the application of Article 8 (1) and that the term "private life" must not be interpreted restrictively[186]. The ECtHR also concluded that a card which was "*filled in on the applicant on which it was stated that he was a 'contact with the Russian embassy' and did 'business of various kinds with the [A.] company'*" included details which undeniably amounted to data relating to the applicant's "private life" and that Article 8 was applicable in this regard[187].

[181] *Gaskin v. The United Kingdom* App No 10454/83 (ECtHR, 7 July 1989).
[182] Ibid para 36.
[183] Ibid (n 181) para 37.
[184] Ibid (n 181).
[185] *Amann v. Switzerland* App No 27798/95 (ECtHR, 16 February 2000).
[186] Ibid para. 65.
[187] Ibid (n 185) para. 66 – 67.

Subsequently in *Rotaru v. Romania*[188] the ECtHR held that "*public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past*"[189], including the right to protection of data processed by the State within Article 8. The collection of data relating to an individual's professional income, with a view to communicating it to third parties, was also considered to fall within the scope of Article 8 in *Rechnungshof v. Osterreichischer Rundfunk*[190]. Kranenborg[191] notes that the ECtHR "*excludes from the privacy scope the processing (which also includes the disclosure) of data: which are not private in itself, and which are not systematically stored images or sound recordings, or other data, which are not systematically stored with the focus of the data subject, and when the data subject could reasonably expect the processing (disclosure).*"[192]

Roagana[193] also notes that the Court never provides a clear and precise definition of what constitutes "private life", only supplying a non-exhaustive list of instances which are deemed to fall within its scope through its case law. To date, the situations considered as falling within the realm of private life include the protection of one's image or reputation; awareness of family origins; physical and moral integrity; sexual and social identity; a healthy environment; protection from search and seizure and privacy of telephone conversations[194], all of which have been applied in respect of living individuals.

[188] *Rotaru v. Romania* App No 28341/95 (ECtHR, 4 May 2000).
[189] Ibid para 43.
[190] Joint cases C-465/00 and C-138/1 *Rechnungshof v. Osterreichischer Rundunk and Others* [2003] ECR I-4948.
[191] H. R. Kranenborg, *Access to Documents and Data Protection in the European Union – On the Public Nature of Personal Data* (Kluwer, 2007).
[192] Ibid 311.
[193] I. Roagana, 'Protecting the right to respect for private and family life under the European Convention on Human Rights' in Council of Europe Human Rights Handbooks (Strasbourg, 2012) 12.
[194] Ibid.

2.2.2 European Court of Human Rights Case-Law

The topic of whether human rights continue to apply following the death of an individual has been touched upon by the ECtHR on a few instances. In *Jaggi v. Switzerland*[195] the "*right of the deceased, deriving from human dignity, to protect his remains from interferences contrary to morality and custom*"[196] was raised. The Court referred to and reiterated the decision in *Estate of Kresten Filtenborg Mortensen v. Denmark*[197] in which it had found that "*the private life of a deceased person from whom a DNA sample was to be taken could not be adversely affected by a request to that effect made after his death*"[198].

In *Estate of Kresten Filtenborg Mortensen v. Denmark* the Government argued that "*the application lodged by KFM's* [Kresten Filtenborg Mortensen] *estate under Article 8 of the Convention was incompatible ratione materiae, in that the notion of 'private life' within the meaning of the said provision related to the circumstances of living individuals, as opposed to a corpse, which could hardly have a 'private life'.*"[199] The Estate of KFM counter-argued that the deceased had a right to rest in peace and to object to KFM's corpse being exhumed and that these rights could only be invoked after KFM's death[200]. The Court recalled a number of cases which dealt with the right of survivors to respect for private and family life in regard to the death of an

[195] *Jaggi v. Switzerland* App No 58757/00 (ECtHR, 13 October 2006).
[196] Ibid para. 19.
[197] *The Estate of Kresten Filtenborg Mortensen v. Denmark* App No 1338/03 (ECtHR, 15 May 2006).
[198] Ibid para. 42.
[199] Ibid (n 197).
[200] Ibid (n 197).

individual[201]. However it distinguished the current case from those recalled in that this one alleged that the violation of the right to respect for private and family life arose after the death of the individual. It then concluded that it was *"not prepared to conclude that there was an interference with KFM's right to respect for private life within the meaning of Article 8 (1) of the Convention*" and the application was deemed inadmissible[202].

In *Akpinar and Altun v. Turkey*[203] the applicants alleged a violation of Article 3 of the ECHR[204] on account of the infliction of torture on their relatives' bodies, either before or after their deaths[205]. The Court held that it had never applied Article 3 in the context of disrespect for a dead body and that it found that "*human quality is extinguished on death and, therefore, the prohibition of ill-treatment is no longer applicable to corpses*"[206]. It hence found that there had been no such violation. Judge Fura-Sandstrom issued a partly dissenting opinion on this case[207], arguing that the "*gratuitous desecration of a corpse, as distinct from scientific tests authorized by a court in the reasonable interests of a third party, is a clear affront to human dignity in breach of Article 3 of the Convention.*"[208]

[201] In particular the Court recalled the cases of *Pretty v. The United Kingdom* App No 2346/02, (ECtHR, 29 April 2002); *Pannullo and Forte v. France* App No 37794/97 (ECtHR, 30 October 2001); and *Znamenskaya v. Russia* App No 77785/01 (ECtHR, 2 June 2005).
[202] Ibid (n 197).
[203] *Akpinar and Altun v. Turkey* App No 56760/00 (ECtHR, 27 February 2007).
[204] Article 3 of the ECHR reads "No one shall be subjected to torture or to inhuman or degrading treatment or punishment."
[205] Ibid (n 203) para. 62.
[206] Ibid (n 203) para. 82.
[207] Ibid (n 203), Partly dissenting opinion of Judge Fura-Sandstrom.
[208] Ibid para. 3.

In her opinion the Judge based her reasoning on the lines that the respect towards and protection of an individual's human dignity and bodily integrity cannot be deemed to end with his death[209]. A resemblance is also drawn between the scope of Article 3 of the ECHR and that of the German Constitution which puts human dignity at the centre of all rights. On this point, the Judge provides the German *Mephisto* case[210] as an example where the "*the dead – particularly those in living memory – remain in communication with the living and we, the living, owe them continuing honour and respect.*"[211] The Judge concludes her opinion by acknowledging that there is no common European standard on the approach to death and she suggests that this may potentially have been one of the reasons discouraging the other judges from extending the protection of Article 3 to deceased persons[212].

To conclude, although Article 8 ECHR contains some elements of the right to data protection, it has not yet been interpreted to grant any protection to the deceased, and data protection in particular. Henceforth, the ECHR does not expressly protect personal data, and much less provides for post-mortem data protection.

[209] Ibid (n 207) para. 4 - 5.
[210] Mephisto, Bundesverfassungsgericht [BVerfG], German Federal Constitutional Court, 1971. The facts of the case were as follows: Klaus Mann published a satirical novel entitled 'Mephisto' which depicted his brother-in-law as favouring the Nazi leaders. The German courts found that the novel dishonoured the good name and memory of the brother-in-law who was deceased.
[211] Ibid (n 207) para. 6.
[212] Ibid (n 207) para. 9.

3. DATA PROTECTION UNDER EU LEGISLATION

3.1 Data Protection Directive

This section shall assess the Data Protection Directive from two main angles: Section 3.1.1 shall deal with the definition of "personal data" and that of "data subject"; and Section 3.1.2 shall go into the practicality of conferring data protection rights on the deceased.

3.1.1 What falls within the remit of the Data Protection Directive?

The Article 29 Data Protection Working Party[213] has held that the construction of a common definition of the notion of personal data will determine what falls within the scope of data protection rules[214]. The author shall hence conduct an assessment of the definition of "personal data" as this is employed in the Data Protection Directive in order to determine whether it includes data pertaining to deceased individuals.

"Personal data" is defined as:

> *"any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*[215]

[213] The Article 29 Data Protection Working Party has an advisory status and acts independently from the institutions of the EU. Opinions issued by it do not reflect the position of other EU institutions and do not have a binding nature.
[214] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20th June 2007.
[215] Article 2 of the Data Protection Directive (emphasis added).

Three main key words are assessed by the Article 29 WP: "relating to", "identified" and "identifiable". In a previous opinion[216], the Article 29 WP held that data is considered to relate to an individual "*if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*". The term "identified" is defined by the Article 29 WP as the instance when a natural person is distinguished from other members of a group of persons; and the term "identifiable" as the instance when, despite a person has not yet been identified, it is possible to do so[217].

The Article 29 WP has also held that identification is normally achieved through particular pieces of information known as "identifiers". Examples of identifiers are considered to be contained in the definition of "personal data"[218] where this states that "*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*"[219]. According to Recital 26 of the Data Protection Directive, in order to determine whether a person is identifiable, all the means likely reasonably to be used to identify such person must be taken into consideration. In this regard, the Article 29 WP has considered data such as video surveillance and IP addresses as constituting data relating to an identifiable person[220].

The term "data subject" is defined within the definition of "personal data" as an "*identified or identifiable <u>natural person</u>*"[221]. The Article 29 WP notes that civil law adopted by Member States

[216] Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN WP 105, 19th January 2005.
[217] Ibid (n 214).
[218] Ibid (n 214).
[219] Ibid (n 35).
[220] Ibid (n 216). See Examples 14 and 15.
[221] Ibid (n 35), emphasis added.

tends to view the notion of natural person as a concept of personality of human beings. Personality is considered to be the capacity to be subject to legal relations, starting from birth and ending at death of the individual[222]. As regards the applicability of the data protection regime, the Article 29 WP concluded that:

> *"Personal data are therefore data relating to identified or identifiable living individuals in principle… Information relating to dead individuals is therefore in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in civil law."*[223]

McCallig[224] contends that the inclusion of the term "natural person" was originally intended to exclude legal persons from the protection offered by the Data Protection Directive. The resulting exclusion of deceased persons through the use of the term "natural person" may have been a mere consequence rather than an intentional act. In light of the time in which the Data Protection Directive was drafted – a time where the internet was still in its early years and data storage was a much greater issue than it is today – it is possible that deceased persons were left out of the scope of the Data Protection Directive because there was no actual need for it. Almost two decades and several developments in the data processing field later, the situation remains unchanged. However, this time round, the theory that this exclusion is simply a consequence is much less plausible. Is it possible that what started off as an oversight has now become a conscious decision to exclude deceased persons from protection?

[222] Ibid (n 214).
[223] Ibid (n 214).
[224] D. McCallig, 'Post-Mortem Privacy: Exploring Deceased's Privacy in a Digital World', in Computers, Privacy and Data Protection Conference, Brussels, 24th January 2014.

3.1.2 Assessing the Practicality of Providing Post-Mortem Data Protection in the Data Protection Directive

As in the case of the Charter of Fundamental Rights of the European Union, the spirit of the law in the Data Protection Directive also helps to shed some light onto the matter. A number of provisions within the Data Protection Directive seem to hint that there exists an implicit requirement for the data subject to be a living human being. In particular, the Data Protection Directive gives substantial importance to the notion of consent. The attainment of the data subject's consent is listed as one of the criteria for attainment of permission for the processing or transfer of data, or as a qualification for an exception from a general prohibition from the processing of sensitive data[225]. While consent can be given pre-emptively to cater for instances where personal data may need to be processed after death, the actual act of giving consent can only be performed by the data subject during his lifetime. At the point of giving consent, the data subject must hence necessarily be alive. The fact that the Data Protection Directive presents the data subject as being in a position where he is able to give consent seems to imply that there is a presupposition the data subject is a living individual.

Other instances where the processing of data is permitted is in the event that certain positive actions are taken by the data subject. For instance, the Data Protection Directive contemplates situations where the data subject launches a request prior to entering into a contract[226] and where the data subject manifestly makes data public[227]. In order to take such actions, the data subject must

[225] Articles 7 (a), 8 (2) (a), 8 (2) (d), 26 (1) (a) of the Data Protection Directive.
~~Article 7 (b) of the Data Protection Directive.~~
~~Article 8 (2) (e) of the Data Protection Directive.~~

necessarily be alive. It is irrelevant whether the effects of these positive actions happen to take place only after death, or whether the data subject would have taken these actions specifically intending them to take effect after he passes away. The focus here is on the manner in which the Data Protection Directive portrays the data subject – as an individual who is able to take certain positive actions which could not be taken once that individual passes away. Therefore, once again, it seems that there is a presupposition that the data subject is a living individual.

The Data Protection Directive also contains a number of provisions which impose obligations on the data controller vis-à-vis the data subject. The nature of the rights awarded to the data subject indicates that the data subject must be a living individual, as otherwise he would not be able to benefit from them. Specifically:

- the data controller must provide the data subject with certain information, the nature of which tends to depend on whether the data was obtained from the data subject or otherwise, such as the identity of the controller and the purposes for which the data shall be processed[228];
- the data subject is granted the right to obtain from the data controller information about the processing of his data, such as the purpose for processing and the categories of data concerned; information about the data undergoing processing and their source; and information on automatic processing of data concerning him, where applicable[229];
- the data subject has the right to object to the processing of data relating to him in certain specified cases[230];

[228] Articles 10 and 11 of the Data Protection Directive.
[229] Article 12 (a) of the Data Protection Directive.
[230] Article 14 of the Data Protection Directive.

- the data subject is also granted the right not to be subject to a decision which may affect him where the decision is based on automated processing of data intended to evaluate aspects such as the data subject's performance at work[231].

It therefore seems that the Data Protection Directive only goes so far so as to provide protection during the lifetime of an individual and data of deceased persons is not within the scope of protection.

3.2 Proposed General Data Protection Regulation

While the provisions of the Data Protection Directive are still very relevant today, the differences in the manner that Member States have implemented it have led to an uneven level of protection throughout the Community[232]. Furthermore, the data protection regime and its rules are in need of some updating in order that they may reflect and adequately address the technological developments which we are experiencing nowadays[233]. As a result, a reform is currently being undertaken in the data protection camp, with the aim of establishing new rules which are "*future-proof and fit for the digital age*"[234]. In this section, the author shall examine the proposed General Data Protection Regulation with a view to seeing whether it includes data of deceased individuals within its scope of protection.

[231] Article 15 (1) of the Data Protection Directive.
[232] European Commission Factsheet, *Why do we need an EU data protection reform?*, accessed via http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf on 18th June 2014.
[233] Ibid.
[234] Ibid.

Section 3.2.1 seeks to set out background information on the status of the reform to the data protection regime. Section 3.2.2 will assess the scope of the proposed General Data Protection Regulation. Section 3.3.3 shall delve into the definitions of "personal data" and "data subject" as these are provided for in the different drafts of the proposed General Data Protection Regulation. Section 3.3.4 closes off this part by assessing the practicality of applying post-mortem data protection rights through the provisions of the different drafts of the proposed General Data Protection Regulation.

3.2.1 Status of the Reform

The first draft of the proposed General Data Protection Regulation was put forward by the Commission in January 2012[235]. In June 2012, in the light of written comments provided by Member States, the Presidency of the Council revised the draft regulation proposed by the Commission[236]. In October 2013, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted on the first reading and a committee report[237] was tabled for plenary in November 2013. In March 2014 the European Parliament voted on its position and decided on a revised version of the text[238]. During its meeting of the 5th and 6th June 2014, the Council reached a partial general approach on specific aspects of the draft General Data Protection Regulation[239]. On the 8th

[235] A copy of the first legislative proposal can be accessed via http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

[236] See Note from the Presidency to the Working Party on Data Protection and Exchange of Information, 22nd June 2012 accessed via http://amberhawk.typepad.com/files/blog_june2012_eu-council-revised-dp-position.pdf on 18th June 2014.

[237] A copy of the report can be accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN.

[238] The text can be accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20140312+ITEMS+DOC+XML+V0//EN&language=EN#title6.

[239] See Press Release on the 3319th Council meeting, Justice and Home Affairs, Luxembourg, 5th and 6th June 2014 accessed via http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/143119.pdf on 23rd July 2014.

and 9th July 2014 the Informal Justice and Home Affairs Ministers Meeting addressed one of the pending issues on whether the proposed General Data Protection Regulation would continue to cover the public sector/service. It was concluded that the draft text addressed most of the concerns regarding the public sector; that further work would be done to address outstanding concerns; and that the draft General Data Protection Regulation would cover data protection within the public sector/service[240].

At the time of writing of this thesis, draft texts have been issued by the Lithuanian Presidency and the Greek Presidency, with the latest version issued in June 2014[241]. However Council negotiations are still ongoing, with Justice Minister Andrea Orlando stating that "*we will try to achieve a common approach during the Presidency*"[242]. The evaluation in question shall be conducted in respect of:

- the text adopted by the European Parliament's legislative resolution of the 12th March 2014 (Parliament's March 2014 draft); and
- the text of the last version of the draft by Council submitted by the Greek Presidency on 30th June 2014 (Council's June 2014 draft).

The assessment shall only be conducted in respect of provisions of the proposed General Data Protection Regulation which have an effect on the determination of whether data qualifies for protection or otherwise. Any provisions which do not have such an effect are beyond the scope of this assessment.

[240] Information obtained through communications with Mr Olav Attard, Research Officer at the Justice and Home Affairs Unit, Permanent Representation of Malta to the European Union on 28th July 2014.
[241] A copy of this draft can be accessed via http://www.statewatch.org/news/2014/jul/eu-council-dp-reg-11028-14.pdf.
[242] See http://www.europarl.europa.eu/news/de/news-room/content/20140722IPR53208/html/Italian-Presidency-priorities-discussed-by-EP-committees accessed on 31st July 2014.

3.2.2 Data Protection under the Reform: The Scope of the Proposed General Data Protection Regulation

In the original version of the legislative proposal of the General Data Protection Regulation put forward by the Commission, Recital 23[243] expressly excluded the data protection regime from applying to deceased persons. This exclusion was retained, albeit with a slight amendment, in the text of the Council's June 2014 draft which reads:

> "*The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person.*"[244]

This exclusion however did not make its way through to the Parliament's March 2014 draft, Recital 23 of which states:

> "*The principles of data protection should apply to any information concerning an identified or identifiable natural person…The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.*"[245]

---

[243] "The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual, unless this would involve a disproportionate effort in terms of time or technical or financial resources. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. The principles of data protection should not apply to deceased persons."

[244] Recital 23 of the draft General Data Protection Regulation as submitted by the Council in June 2014. See Ibid (n 243).

[245] See Amendment 6 to the proposed General Data Protection Regulation resulting from the European Parliament legislative resolution of 12th March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading) accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

The Council seems eager to expressly exclude data of deceased persons from the scope of protection to be conferred by the proposed General Data Protection Regulation. On the other hand, the Parliament, while not specifically including data of deceased persons within the scope, shies away from an express exclusion. The reason for this difference in approach is not clear; however it seems that from the Council's side, pressures may have been placed by Sweden to put this exclusion in place.

3.2.3 Definitions of "personal data" and "data subject"

As regards the definition of the term "data subject", which is contained in the definition of "personal data", the Parliament's March 2014 draft reads:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person"*[246]

//EP//TEXT+TA+20140312+ITEMS+DOC+XML+V0//EN&language=EN#title6 on 18th June 2014, emphasis added.

[246] See Amendment 98 to the proposed General Data Protection Regulation resulting from the European Parliament legislative resolution of 12th March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading) accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20140312+ITEMS+DOC+XML+V0//EN&language=EN#title6 on 18th June 2014, emphasis added.

The Council's June 2014 draft is identical to the Parliament's March 2014 draft insofar as it relates to the data subject being referred to as a "natural person"[247]. Recital 125(a) of the Council's June 2014 draft also expressly excludes data of deceased individuals from the application of the data protection regime, stating:

> *"…Where personal data are processed for archiving purposes in the public interest, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons, unless information on deceased persons impinges the interests of data subjects."*[248]

The same wording in regard to data of deceased persons is applied in Recital 126(a)[249] of the Council's June 2014 draft which relates to the processing of personal data for historical purposes[250]. The note to this Recital is rather interesting and states: "*ES and MT thought that it was repetitious to refer to the non-application to deceased persons (also e.g. in recital 126, end first paragraph). MT added that certain sensitive data of deceased could be interesting, for example it would be interesting for a child to know if a deceased parent had a certain illness. MT suggested to add text like "if it did not impinge the interests of other data subjects". Support from*

[247] The definition of "personal data" under the Council's June 2014 draft reads: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." Differences can be seen in the definition of what constitutes an identifier; however both definitions refer to the data subject as a "natural person".

[248] Ibid (n 243), Recital 125(a). The note to this Recital is also interesting: "ES and MT thought that it was repetitious to refer to the non-application to deceased persons (also e.g. in recital 126, end first paragraph). MT added that certain sensitive data of deceased could be interesting, for example it would be interesting for a child to know if a deceased parent had a certain illness. MT suggested to add text like "if it did not impinge the interests of other data subjects". Support from EE and SK to the MT suggestion. SK suggested alternatively drafting on the lines that data on deceased persons linked to living persons could be used."

[249] Recital 126(a) states "Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased person, unless information on deceased persons impinges the interests of data subjects."

[250] Ibid (n 243) Recital 126(a).

EE and SK to the MT suggestion. SK suggested alternatively drafting on the lines that data on deceased persons linked to living persons could be used."

It seems that there is an internal struggle within the Council on this point. While some Member States want to expressly exclude post-mortem data protection, others feel that the processing of data of deceased persons could be of value and prefer to afford a limited degree of protection thereto. Malta's suggestion to retain the exclusion of post-mortem data protection, but only insofar as the processing of data of the deceased does not impinge of the interests of data subjects, seems to further imply that data subjects are viewed solely as living individuals. Furthermore, this consideration is in line with the arguments to be presented in this thesis, mainly that the processing of data of deceased persons can pose a risk to living individuals.

3.2.4 Assessing the Practicality of Providing Post-Mortem Data Protection in the Proposed General Data Protection Regulation

While the Parliament's March 2014 draft does not expressly exclude the application to data of deceased individuals, the spirit of the law seems to imply this nonetheless. In providing the instances in which the processing of data is permitted the Parliament's March 2014 draft includes the attainment of the data subject's consent[251], the necessity to process data upon request of the data subject prior to entering into a contract[252], and instances where the data subject makes the data manifestly public[253]. In addition to this, the conditions of consent indicate that the data subject has the right to withdraw his consent at any time[254]. Once again, the manner in which the data

[251] Articles 6 (1) (a), 9 (2) (a), 9 (2) (d) of the proposed General Data Protection Directive (Parliament's March 2014 draft).
[252] Article 6 (1) (b), 9 (2) (aa) of the proposed General Data Protection Directive (Parliament's March 2014 draft).
[253] Article 9 (2) (e) of the proposed General Data Protection Directive (Parliament's March 2014 draft).
[254] Article 7 (3) of the proposed General Data Protection Directive (Parliament's March 2014 draft).

subject is presented seems to pre-suppose that the data subject is a living individual. A deceased person is not able to give his consent, lodge requests, enter into contracts or make data public. In some cases, these actions may be taken by the data subject during his lifetime, only to become effective after his death. However, the author believes that the issue of whether the implications of these actions takes place during the lifetime of the data subject or thereafter is irrelevant to the assessment of what constitutes a data subject. In understanding the legislator's intentions one must view the data subject as presented by the law – in this case, he is presented as being able to take certain actions which a deceased person would not be able to take. Applying some of the provisions of the Parliament's March 2014 draft to a deceased person in the shoes of the data subject is not a workable option.

In addition to the above, the Parliament's March 2014 draft also provides the data subject with a number of rights which include, inter alia, "*the provision of clear and easily understandable information regarding the processing of his or her personal data, the right of access, rectification and erasure of their data, the right to obtain data, the right to object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation*"[255], all of which require action on the part of the data subject, once again implying that he is a living individual. The Parliament's March 2014 draft also provides for the communication of a personal data breach to the data subject[256] and grants data subjects the right to contact the data protection officer on issues relating to the processing of his data and to request exercising his rights[257].

[255] Article 10a of the proposed General Data Protection Directive (Parliament's March 2014 draft).
[256] Article 32 of the proposed General Data Protection Directive (Parliament's March 2014 draft).
[257] Article 35 (10) of the proposed General Data Protection Regulation (Parliament's March 2014 draft).

The data protection reform is still a work-in-progress and the shape which the final General Data Protection Regulation will eventually take place is still unknown. We have seen how the draft versions put forward by the Parliament and the Council have taken separate routes in dealing with data of deceased persons. In terms of scope of the proposed General Data Protection Regulation, the Council's draft expressly excludes protection from being conferred onto data of the deceased as a general rule. However, it seems that the Council is willing to allow for a few exceptions, mainly where the processing of data of the deceased can affect living individuals. The Parliament's version is more silent on whether data of deceased persons is within the scope of the reform when stating its scope. In terms of definitions and portrayal of the data subject, and the application of the regime, both drafts seem to presuppose that the data subject is a living individual, presenting him as a person who is able to perform certain positive actions. At the time of writing of this thesis, it is too early to determine which of the two routes will prevail and what will be the final outcome. However, it seems quite unlikely that a specific inclusion of post-mortem data protection can be expected.

4. DATA PROTECTION UNDER NATIONAL LEGISLATION

The mandate of the Data Protection Directive requires Member States to bring into force laws for the compliance with its provisions on a national level[258]. Notwithstanding this, in the *Lindqvist* case[259], the European Court of Justice held that "*nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not*

[258] Article 32 of the Data Protection Directive.
[259] Case C-101/01 *Criminal Proceedings against Lindqvist* [2003] ECR I-12971.

included in the scope thereof provided that no other provision of Community law precludes it"[260]. Member States are therefore able to tailor their national laws on data protection in such a way so as to go beyond the level protection contemplated in the Data Protection Directive. As previously established, the jurisdictional scope of this thesis shall be restricted to the legal system of the European Union. However, in an effort to understand the approach being taken by individual Member States in regard to the treatment of data in a post-mortem stage, the author has chosen to briefly assess a few national data protection laws.

For the most part, national laws of Member States stick quite closely to the wording of the Data Protection Directive. The majority of national laws of Member States refer to the data subject as an identified or identifiable natural person[261] or a natural person to whom personal data relates[262] with some slight variances such as in the case of the Italian Personal Data Protection Code[263] which defines "data subject" as any natural or legal person, body or association that is the subject of the personal data[264] and Spanish data protection law[265] which refers to the data subject as the natural person who owns the data undergoing the processing[266].

[260] Ibid, para 98.
[261] See for instance: Act on Protection of Personal Data (Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll.), Slovakia; Republic of Lithuania Law on Legal Protection of Personal Data (21 January 2003, No. IX-1296); and The Act on Processing of Personal Data (Act No. 429 of 31 May 2000 as amended by section 7 of Act No. 280 of 25 April 2001, section 6 of Act No. 552 of 24 June 2005 and section 2 of Act No. 519 of 6 June 2007), Denmark.
[262] See for instance: Data Protection Act, 15th July 2003 (Chapter 440 of the Laws of Malta); Personal Data Protection Act (Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts), Czech Republic.
[263] Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003, Italy.
[264] Ibid, Section 4 (1) (i).
[265] 23750 Organic Law 15/1999 of 13 December on the Protection of Personal Data, Spain.
[266] Ibid, Article 3 (e).

On the other hand, a number of Member States have opted to expressly include or exclude the applicability of their data protection regime following death of the data subject. In particular, the Bulgarian Data Protection Act[267] allows the heirs of the data subject to exercise his rights to access and attainment of information in the event of the data subject's death[268]. French data protection law[269] takes on a similar approach, enabling heirs of a deceased person to demand that data controllers update the data they hold about the deceased data subject to reflect the death[270]. Furthermore, as a general rule, data relating to a deceased person may continue being processed after his death, unless he has expressed his refusal to such processing in writing before his death[271].

Slovenia dedicates an entire proviso of its Personal Data Protection Act[272] to the protection of personal data of deceased individuals, which holds that data controllers may only supply data on deceased individuals to data recipients authorized to process personal data by statute and the legal heirs of the deceased data subject (upon their request and unless the deceased individual prohibited this in writing before his death). Data of deceased persons may also be provided by the data controller to any persons intending to use it for historical, statistical or scientific-research purposes, unless the deceased data subject or his heirs prohibit it[273].

[267] Personal Data Protection Act Promulgated State Gazette No. 1/4.01.2002, effective 1.01.2002, supplemented, SG No. 70/10.08.2004, effective 1.01.2005, SG No. 93/19.10.2004, No. 43/20.05.2005, effective 1.09.2005, amended and supplemented, SG No. 103/23.12.2005, amended, SG No. 30/11.04.2006, effective 12.07.2006, Bulgaria.
[268] Ibid, Article 28 (3).
[269] Act Of 6 August 2004 Relative To The Protection Of Individuals With Regard To The Processing Of Personal Data.
[270] Ibid, Article 40.
[271] Ibid (n 274), Article 56.
[272] Personal Data Protection Act of the Republic Of Slovenia (No. 001-22-148/04), 15th July 2004.
[273] Ibid, Article 23.

The United Kingdom has opted for a contrary approach, defining "personal data" as "*data which relate to a living individual who can be identified*"[274], expressly excluding the applicability of its Data Protection Act following the death of the data subject. Sweden adopts a similar attitude, limiting its data protection regime to "*all kinds of information that directly or indirectly may be referable to a natural person who is alive*"[275].

5. OBSERVATIONS

The wording of both the Charter of Fundamental Human Rights and the European Convention on Human Rights seems to imply that the right to data protection and the right to private life can only be applied throughout the lifetime of an individual. Furthermore, case-law of the European Court of Human Rights tends to support this view. As Judge Fura-Sandstrom indicated, the fact that there is no established standard as to how to deal with matters of death in the human rights field may keep the Court from ruling in favour of awarding rights to the deceased. Judge Fura-Sandstrom bases her arguments in favour of extending the applicability of the right to private life beyond death of the individual on the notions of human dignity and preservation of the quality of life. These arguments are likely to be considered well-founded in jurisdictions where human dignity plays a central and constitutional role, such as Germany. However, they may be less viable in other venues.

Moreover, the human dignity argument is mainly geared at extending the applicability of the right to private life, and data protection, in the interests of the deceased. This may be in line with the

[274] Data Protection Act, 16th July 1998, Article 2 (e), emphasis added.
[275] Personal Data Act (1998: 204), Sweden, 29th April 1998, Section 3, emphasis added.

claims being brought in current literature on post-mortem data protection; however they tend to waiver in significance when applied to the prevention of data processing harms to living individuals. The author does not believe that the extension of applicability of the right to private life as a whole can be justified by the protection against the threats to personal autonomy that big data companies pose to living indviduals. The granting of human rights to an individual is intended to safeguard his basic and fundamental interests, and not those of third parties. Therefore extending the entire right to private life to also apply after death, simply to safeguard other (still living) individuals' personal autonomy seems to be taking a step too far.

As regards the Data Protection Directive and the proposed General Data Protection Regulation, there do not seem to be any apparent efforts to cater for post-mortem data protection specifically. While there is no express exclusion in the Data Protection Directive, the wording used and the spirit of the law tend to imply that post-mortem data protection is not within its scope. The Article 29 WP has made it clear that in its opinion, the Data Protection Directive does not contain post-mortem data protection within its scope. Opinions of the Article 29 WP are not binding and merely advisory; however they tend to shed light onto the intentions of the legislator and give useful guidance on the manner in which data protection laws should be interpreted. At best, the text of the Data Protection Directive can be said to be unclear and ambiguous when it comes to post-mortem data protection. There is no express inclusion thereof, and the spirit of the law seems to drift away from this notion.

The text of the proposed General Data Protection Regulation is not yet final and it is still unclear what shape it will take when it is concluded. The Parliament and Council seem to be taking

different directions in their approach towards post-mortem data protection and it cannot be determined at this stage which of the two shall prevail in final negotiations. If the version adopted by the Council were to succeed, an express exclusion of post-mortem data protection will be imposed, potentially with some exceptions. On the other hand, the Parliament's version, while not expressly excluding post-mortem data protection, does not seem to cater for it either. Therefore, it seems that regardless of which of the two makes it through to the final draft, it is unlikely that post-mortem data protection will be explicitly included in the EU data protection regime in the near future.

On a Member State level, the approach towards post-mortem data protection is far from harmonized. While the national laws of some Member States go the extra mile to ensure that the deceased still benefit from data protection, others specifically exclude such protection from being afforded. The fact that Member States are able to vary to these extents in their regulation of post-mortem data protection signifies the ambiguity circling this notion within the Data Protection Directive. Since the Data Protection Directive is silent on the matter, offering only implicit hints towards the exclusion of post-mortem data protection, Member States have been able to go a step further and specify expressly whether or not this concept shall exist in their jurisdiction.

Chapter IV

Is the Distinction between Data of Deceased and Living Individuals Justified?

1. SCOPE AND PURPOSE

In Chapter I we have seen how the application of big data predictions is capable of putting individuals' personal autonomy at risk. We have also seen that this threat to personal autonomy is exactly one of the harms of data processing which data protection aims to safeguard individuals from[276]. In Chapter II we saw that the big data companies tend to process data pertaining to both living and deceased individuals. The assessment carried out in Chapter III resulted in the conclusion that data pertaining to deceased individuals is however not covered by data protection law across the EU. This brings us back to the central research question which this thesis aims to address:

> *In the age of big data and its threat to personal autonomy, should it matter if the data pertains to living or deceased individuals for the purposes of data protection?*

This chapter aims to carry out two exercises:

- It seeks to understand the reasoning behind the distinction made by the data protection regime between data of living and deceased individuals by identifying potential justifications for the exclusion of post-mortem data protection; and
- It shall evaluate whether these alleged justifications also apply in the age of big data, where the processing of data pertaining to both living and deceased individuals poses a risk to individuals' personal autonomy.

[276] Ibid (n 26) 41.

2. UNDERSTANDING THE EXCLUSION OF POST-MORTEM DATA PROTECTION

One must keep in mind that the boom in the data collection and processing industry[277] is relatively recent. Prior to this, the issues that the longevity of data brings with it were practically non-existent. We are in a situation where technological developments have pushed forward data collection and processing activities, but the regulation of these activities is lagging behind[278]. This may be one of the reasons why post-mortem data protection is not contemplated by the Data Protection Directive; however it does not explain why data of deceased persons seems to still being left out of the scope of the proposed General Data Protection Directive. Throughout this section the author shall present reasons which may explain why a distinction is applied.

2.1 Data of the Deceased may still Receive Indirect Protection

A point raised by the Article 29 WP is that, despite the fact that data relating to deceased individuals is not covered by data protection rules, it may still indirectly receive protection in certain cases. In its Opinion[279] the Article 29 WP identifies four instances where data enjoy post-mortem protection:

[277] As at 10th February 2014, Bloomberg records 108 public companies having data processing and management as their primary business model, 39 of which are established within the European Union. See http://www.bloomberg.com/markets/companies/data-processing-mgmt/.
[278] J. Lingel, *The Digital Remains: Social Media and Practices of Online Grief* (The Information Society, 2013) 190 – 195.
[279] Ibid (n 214).

2.1.1 The data controller may not be in a position to ascertain whether the individual to whom the data pertains is living or deceased

As we have seen in Chapter I, data controllers face difficulties in becoming aware of the death of their users. Insofar as the data controller has no reason to believe that the data subject has passed away, it shall continue to treat the data as pertaining to a living individual. It will hence process the data as per the data protection rules nonetheless. Another point raised by the Article 29 WP in this regard is that, even when the data controller is aware that the individual is deceased, it may be easier to apply the same rules to all data held by it, rather than to distinguish between data of living and deceased individuals. Filtering data according to the status of its subject and applying different methods of processing according to data types is time and resource consuming. The benefit derived therefrom may not be worth the effort. As a result, data may continue to receive the protection to which it was eligible when its subject was still alive.

2.1.2 Data referring to a deceased individual may simultaneously refer to a living individual, rendering it to still fall within the scope of data protection rules

Data about an individual may sometimes also relate to a third party, for instance health data about a mother may also relate to her offspring due to genetics[280]. Another example is where data contained in a user's social media profile refers to other persons through tagging systems. As long as the data relates even in part to a living individual, it shall continue to enjoy the protection conferred to data pertaining to living individuals.

[280] Ibid (n 214) 22.

2.1.3 Certain types of data enjoy protection due to confidentiality obligations

Data about an individual may be subjected to confidentiality obligations, for instance through non-disclosure agreements or due to other secrecy obligations. In particular, data held by data controllers who also form part of a profession, for instance doctors or lawyers, will be protected by professional secrecy under national laws of Member States. These obligations continue to apply even after the death of the individual they pertain to[281]. Nonetheless, one must keep in mind that confidentiality obligations are not part of the data protection regime and the majority of companies involved in big data analytics are unlikely to be tied down with confidentiality obligations or professional secrecy. Therefore, while this argument may hold up with regard to data controllers such as law firms, it becomes quite weak when applied to big data companies in general.

2.1.4 Member States may cater for the treatment of data at a post-mortem stage in their national laws

As pointed out in Chapter II, Member States are not precluded from extending the scope of their national data protection laws. We have seen how some Member States have opted to provide protection of data even after the death of the data subject, while others enable the data subject's heirs to exercise the data subject's rights in his stead[282]. This justification is however limited in that it does not apply uniformly throughout all of the EU.

[281] Ibid (n 214).
[282] See Ibid (n 266 – n 280).

2.2 Data is Automatically "Filtered Out" Over Time

When determining whether there is an actual need for post-mortem data protection, one must also consider that data may lose some of its value, in terms of usefulness, once the individual it pertains to passes away. Ambrose[283] argues that time tends to have certain effects on information. In presenting her argument she sets out the presumption that the reasons for which data continues to be processed are that the controller has the interest and resources to maintain it. The value which drives the data controller to process the data lies in the interest in communicating the data, the utility of the data and the interest of the public. As a result, over time interest in information decreases; its use decreases; content stales; information becomes less accurate, less reliable and represents less context[284]. Once a data subject dies, no further data is generated by him. Therefore whatever data he leaves behind may eventually become outdated or useless for the purposes of big data analytics. As a result it may automatically be filtered out of the processing pool by big data companies.

2.3 Impracticality of the Data Protection Rights of the Deceased

From a more practical perspective, as observed in Chapter II, the design and structure of the current data protection regime are such that it is difficult to envisage how it would apply to data pertaining to deceased persons. The data protection regime seeks out its own enforcement by granting rights to data subjects. These rights require positive action on the part of the data subject and hence cannot be taken by a deceased person. Moreover, the Data Protection Directive does not provide

[283] M. Ambrose, *Where has the Time Gone? An Information Life Cycle Approach to the Right to be Forgotten*, in Computers, Privacy and Data Protection Conference, Brussels, 23rd January 2014.
[284] Ibid.

for any instances where these actions can be taken by third parties on behalf of the data subject (for instance by heirs on behalf of the deceased).

While actions taken during the lifetime of the data subject will remain in effect after his death, the data subject is precluded from enforcing his rights after his death. In this regard, the author recognizes that certain actions may be taken pre-emptively by the data subject to cater for instances which may arise after his death. However, as argued earlier, the author believes that this does nothing to alter the manner in which the data subject is presented by the Data Protection Directive. The fact of the matter remains that the Data Protection Directive presents the data subject as a natural person who is able to take certain positive actions – a depiction which is not workable in respect of deceased persons. Therefore, even if protection were to be granted over data pertaining to deceased individuals, the regime would have to be adapted in certain respects for it to function properly. In light of the fact that the proposed General Data Protection Regulation does not seem to include any adaptations of this nature, it seems that the proposed regime would still not be sufficiently adequate to provide post-mortem data protection.

3. DO REASONS FOR THE EXCLUSION OF POST-MORTEM DATA PROTECTION HOLD WATER IN THE AGE OF BIG DATA?

3.1 Indirect Protection: A Solution or a Quick Fix?

As regards the argument that data pertaining to deceased persons may still be given indirect protection in practice, the key word here is "may". The fact that big data companies face difficulties in distinguishing between data of living and deceased individuals, or that they do not bother to filter one type from the other, does not necessarily mean that they will always give due protection to data pertaining to deceased persons. As time goes by, data of deceased persons which simultaneously refers to living individuals, will eventually become data referring solely to deceased persons. Furthermore, the fact that a number of Member States impose post-mortem data protection only goes so far to solve the problem. There still remains a mass of data pertaining to citizens of Member States which do not offer, or expressly exclude, post-mortem data protection, which remains unprotected. Arguments against post-mortem data protection based on the indirect protection that may be allocated to data of deceased persons only hold up temporarily, or in specific circumstances.

3.2 Impracticality of Post-Mortem Data Protection: A Justification or an Excuse?

On the point of enforcement of the data protection regime in respect of data of deceased persons, this merely presents a reason why the Data Protection Directive (and eventually the General Data Protection Regulation) does not constitute the most adequate means to provide post-mortem data protection. Admittedly, the fact that the main legal instrument used to provide data protection in

the EU will not function properly when applied to data post-mortem is a substantial obstacle. However, it does not, in and of itself, justify the exclusion of post-mortem data protection. It simply means that additional work would need to be carried out to find a means to provide post-mortem data protection if this notion were to be introduced.

3.3 Data Protection: More than Mere Informational Privacy

In safeguarding individuals' privacy, data protection seeks to do much more than to merely protect individuals from third party intrusions. It seeks to enable them to realize their full potential in society[285]. The value of personal autonomy, which stems from the right to privacy, is not merely an individualistic value, but one which also has substantial relevance in society[286]. As we have seen in Chapter I, stripping individuals of their freedom of choice and their personal autonomy means to remove a fundamental pillar of the democratic society. Therefore, data protection should not be viewed solely as protecting individuals from the harm which may ensue as a result of the processing of their own data. Data protection also works to protect society as a whole from the harms which the processing of data in general may bring about[287].

When discussing the notion of post-mortem data protection, we must take a step back to be able to see the bigger picture. The threat that big data poses to personal autonomy is a result of the processing of a large pool of data which refers to both living and deceased individuals. Therefore the issue of whether data used in big data analytics pertains to a living or deceased person is

[285] Ibid (n 41) 147.
[286] Ibid (n 45) 378.
[287] F. H. Cate, P. Cullen and V. Mayer-Schonberger, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (Oxford Internet Institute, University of Oxford, March 2014) 14.

irrelevant to the ensuing harm that comes with the act of processing. By distinguishing between data of living and deceased individuals in determining its applicability, the EU data protection regime is arguably only fulfilling its purpose in part. The threat to a data subject's personal autonomy no longer derives solely from the processing of data pertaining to that same data subject. We are in an age where the processing of other people's data can be equally prejudicial to the data subject. The author believes that data pertaining to deceased individuals merits protection not by virtue of the data subject it pertains to, but rather by virtue of the harm its processing may cause to the personal autonomy of individuals in general, and the threat to democracy that this brings with it.

A counter-argument to this could however be that, if data of deceased persons merits protection on the basis of the harm its processing (through big data analytics) may cause to living individuals, would this not be the case for all kinds of data used in big data analytics? Applying this argument across the board would result in claims that any data used in big data analytics, including data which is not personal data, should be awarded protection under the data protection regime. In this regard, the author believes that a distinction should be made between personal data and other types of data. The scope of this thesis is to assess whether a distinction should be made between personal data of living and deceased individuals for the purposes of data protection in light of the risk that big data poses to the personal autonomy of living individuals. It does not purport to delve into a discussion on whether a distinction should be made between personal data and all other data used in big data analytics in light of the same circumstances.

Since its inception, the data protection regime has offered protection specifically for personal data. On the other hand, data which is not capable of identifying or does not relate to an individual has never fallen within the scope of data protection. The main subject under assessment in this thesis is whether data protection should stop being provided upon death; and not whether it should start to apply to different kinds of data which were never within the scope of the regime. Considering that the processing of personal data of deceased persons seems to continue to pose the same risks as it did when the data subject was still alive, the author fails to see why protection cease to be conferred upon death. In light of the above the author is of the opinion that the criteria employed by the Data Protection Directive and the proposed General Data Protection Regulation in determining whether data should be awarded protection need revisiting. The exclusion from protection of data pertaining to deceased persons is not justified and the position should be altered to meet the needs of today's society.

4. SUGGESTIONS FOR THE WAY FORWARD

The scope of this thesis revolves around identifying whether or not a distinction should be made between data pertaining to living and deceased individuals for the purposes of data protection. The findings of this thesis have led the author to the opinion that there is no reason for such a distinction and that the data protection regime should also cater for post-mortem data protection. While it is not within the scope of this thesis to identify how legislators should go about implementing post-mortem data protection, the author has chosen to discuss two potential options briefly. The contents of this section are not aimed at finding a solution, but rather at sparking a discussion on the way forward should post-mortem data protection be introduced into the data protection regime.

4.1 Propertisation of Personal Data

In 2013 Harbinja[288] conducted an exercise to evaluate whether the text of the Data Protection Directive and that of the Commission's original proposal for the General Data Protection Regime[289] protect post-mortem privacy. In examining the proposed General Data Protection Regulation, an assessment was also conducted in respect of the Council's revised version of the text provided in June 2012[290] and the Albrecht Report[291]. Going in line with the findings of Chapter III of this thesis, Harbinja found that the Data Protection Directive "*does not mention deceased's data in any context*."[292] As regards the text of the Commission's proposal, Harbinja notes that, while there is still no reference to data pertaining to deceased individuals, certain novelties introduced through this text tend to "*serve as a base for discussing a potential shift in the EU data protection system and a move towards the property-based regime*."[293] In particular, she refers to the introduction of the right to be forgotten and the right to data portability, which she argues seem to imply the commodification of personal data[294].

[288] Ibid (n 18).
[289] European Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25th January 2012.
[290] Ibid (n 243).
[291] Jan-Philipp Albrecht, a Rapporteur for the European Parliament's Civil Liberties, Justice and Home Affairs Committee, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* 2012/0011(COD), 17th December 2012.
[292] Ibid (n 18) 26.
[293] Ibid (n 18) 28.
[294] Ibid (n 18) 34 – 35.

The text of the Commission's original proposal has since undergone a number of reviews and discussions, with several amendments being proposed. Purtova[295] notes that the control awarded to data subjects in the Commission's original proposal is less than that awarded in the current Data Protection Regime[296]. On the other hand, the text adopted by the Committee on Civil Liberties, Justice and Home Affairs in October 2013[297] provides a wider scope for the control rights awarded to data subjects[298]. The text of the proposed General Data Protection is still the subject of ongoing discussions and negotiations and no final version has been agreed upon by the European Parliament and the Council as of yet. Until the time that such agreement is reached, the level of control rights that will be provided to data subjects may change yet again. Therefore, at this stage it is too early to say that a commodification of personal data is being hinted at by the proposed General Data Protection Regulation. Nonetheless, the author shall look into this option to briefly assess whether it would be capable of constituting a potential candidate for the mechanism implementing post-mortem data protection into the data protection regime.

The propertisation of data model is one employed in the legal system of the US, whereas the EU views data protection from a human rights perspective[299]. Discussions on the propertisation approach could therefore be argued to hardly be relevant to the EU. Notwithstanding this, Purtova[300] argues that this American debate may offer Europe with some guidance and potentially a few lessons to learn from[301]. For instance, the propertisation approach may serve a market, non-

[295] Ibid (n 20).
[296] Ibid (n 20)
[297] Ibid (n 239).
[298] Ibid (n 20) 29.
[299] Ibid (n 18) 29.
[300] N. Purtova, *Property Rights in Personal Data: Learning from the American Discourse* (Computer Law and Security Review, 2009).
[301] Ibid 507.

market or even protective function[302]. Another advantage of the propertisation model over the human rights model, highlighted by Koops[303], is that under the former regime the individual need not prove that harm has been caused. On the other hand, other authors have argued that the propertisation approach will result in less privacy protection[304] and less control for the data subject[305]. Propertisation also raises issues of future transfers of personal data due to free alienability[306] – once the data subject transfers his data to a data controller, the latter can freely transfer it to third parties.

From a post-mortem data protection perspective, the propertisation model would be beneficial because it enables personal data to be handled through probate upon the death of the data subject[307]. This would provide data subjects with the opportunity to determine what happens to their data upon their death, for instance by providing instructions in their will. Personal data of data subjects who die intestate would be transmitted to their heirs according to succession law. This solution may provide answers to questions regarding the access to and management of data pertaining to deceased persons by their survivors. However, it does not automatically require data controllers to process data of deceased persons in line with the principles and rules of data protection. Therefore employing a propertisation approach does not aid in eradicating the distinction established by the data protection regime.

[302] Ibid (n 305) 520.
[303] B. J. Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice* (ScriptEd, 2011) 229 – 256.
[304] See J. E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object* (Stanford Law Review 52, 2000) 1373 – 1426.
[305] See P. Samuelson, *Privacy as Intellectual Property* (Stanford Law Review 52, 1999) 1125 – 1167.
[306] Ibid.
[307] Ibid (n 18) 37.

4.2 Extending the Definition of "Data Subject"

As we have seen in Chapter III, the applicability of the EU data protection regime is determined according to the definition of "personal data" (which contains a definition of "data subject") as adopted in the Data Protection Directive (and eventually the General Data Protection Regulation). An amendment of the definition of "data subject" to also include deceased persons would therefore automatically extend the application of the data protection regime to data pertaining to deceased persons. Harbinja also seems to hint at supporting this approach, suggesting that data pertaining to deceased persons is included within the definition of personal data, "*awarding a time-limited protection, with appropriate safeguards in relation to other relevant interests*"[308].

This solution would enable the data protection regime to incorporate post-mortem data protection and simultaneously continue to be human rights-based. Data protection, as a right, can continue to co-exist with other rights and freedoms, such as the freedom of expression even after the death of the data subject. As regards the limitation of protection by time, this may have been suggested in the interests of proportionality. Data of deceased individuals will eventually become outdated and big data companies are unlikely to process data which does not yield relevant and valid results. At that stage there would no longer be a need for post-mortem data protection. Determining the specific time period would require further research into how long after the data subject's death data is usually processed by big data companies. A further limitation which may be imposed in this regard could potentially be that of granting protection solely to personal data of deceased persons which was collected during their lifetime. This would prevent situations where data of

[308] Ibid (n 18) 38.

long-deceased individuals (possibly constituting historic data) are also deemed to fall within the scope of data protection.

There does exist however one considerable obstacle to this solution. As we have seen in Chapter II, the data protection regime enables its own enforcement by granting rights to the data subjects. A deceased data subject would naturally not be able to exercise his rights. Therefore, while data controllers would technically be required to adhere to data protection rules when processing data of deceased persons, there would be no means for such rules to be enforced. This issue could potentially be solved by allowing the heirs of the deceased to exercise his rights so as to enable the enforcement of data protection rules nonetheless. This is the approach adopted by a number of Member States such as Bulgaria, France and Slovenia[309]. However, the efficacy of relying on heirs of the data subject to exercise his rights, and hence enforce data protection rules is debatable. The heirs of the deceased may feel that since the data subject is deceased there is no need to ensure that his data continues to be protected. Furthermore, since the data does not pertain to them, there is less of an incentive for them to ensure that the deceased's data is being processed in accordance with data protection rules.

4.3 Potential Areas for Further Research

Further research is undoubtedly required in order to properly assess whether either of the suggestions touched upon above would provide an adequate solution to the issue at hand. The conducting of a more in-depth study into manners in which post-mortem data protection may be

[309] See Ibid (n 272 – n 278).

provided could even reveal solutions which are outside of the data protection regime. Stepping away from the traditional method of offering protection could serve to set up a mechanism directed specifically for post-mortem data protection. Rather than trying to adapt an already-existing framework to a relatively new concept, a more "tailor-made" approach may prove to be more effective and easier to implement in practice.

This thesis has been limited in its scope from various aspects, with its main restriction being that its central focus revolved around the distinction between two sets of data (data of the living and data of the deceased) which both fall under the umbrella of personal data in that they are both capable of identifying a specific individual. Notwithstanding this, the author believes that this thesis could potentially provide a starting point into re-evaluating some of the core principles that make up the almost-two-decade-old data protection regime in light of new risks and concerns that the advent of big data has brought with it. The author believes that issues such as whether the distinction between personal data and all other information used in big data analytics is still valid in providing an effective data protection regime would be an interesting area for further research.

Conclusion

Certain basic principles enshrined in the current data protection regime have gone unquestioned for years – so much so that some of these concepts seem likely to survive the reform which is presently taking place. What is the reason behind this silent acceptance of long-standing principles? Is it because they have proved to be a fundamental and effective tool in delivering data protection, or could it be that there simply never was a reason to question their inclusion? We started off this thesis with the question: In the age of big data and its threat to personal autonomy, should it matter if the data pertains to living or deceased individuals for the purposes of data protection? In addressing this question, the author has aimed to seek an understanding as to why a distinction is present, and whether its retention is justified in the era of big data.

Throughout this study we saw how information generated by deceased individuals during their lifetime is being used by big data companies, jointly with information pertaining to living individuals, in a manner which will have an impact on the lives of others. If taken too far, the application of big data analytics, such as through the personalization of services, has the potential of stripping individuals of their freedom of choice and their personal autonomy. The selection process involved in making everyday choices will be performed by big data companies for the individual. As a result, the individual will only be exposed to a limited amount of options, rather than being left to narrow down the options himself. Risks such as the one at hand are aimed to be addressed through data protection rules. The data protection regime aims to regulate the manner in which data is processed by data controllers, to limit as much as possible the harms to individuals and society that may ensue therefrom.

This thesis has aimed to raise awareness as to the need for the introduction of post-mortem data protection in light of the threats that big data has brought about, particularly to individuals' personal autonomy. While it is not the intention of the author to propose a solution for the actual introduction of post-mortem data protection, a few points for the initiation of a discussion on this matter have been provided. Catering for post-mortem data by means of the existing data protection regime would ensure that data of living and deceased individuals can be processed in harmony with each other. The upcoming move from the Data Protection Directive to the proposed General Data Protection Regulation presents an opportunity for ensuring that data protection rules are uniform across all Member States of the EU. However, it seems unlikely that the data protection reform will do much for the introduction of post-mortem data protection.

Notwithstanding the above, the author believes that there is room for further research in this regard. Routes for providing post-mortem data protection need not be grounded in the data protection regime. Further studies may potentially reveal that the notion of big data and the risks it has brought with it are far too big an opponent for the data protection regime to battle. Just as post-mortem data protection would prove helpful in the fight against the harms of big data analytics, protection over additional kinds of data may also do its part. This would imply a great overhaul of the data protection regime, challenging one of the core principles that has formed the basis of data protection since its inception. No such challenges have appeared during in the process the current reform. Perhaps we are not yet ready to go down this path?

Bibliography

Books

Bygrave, L.A., Data Protection Law: Approaching its Rationale, Logic and Limits, Kluwer International, 2002

Claes, E., Duff, A. and Gutwirth, S., Privacy and Criminal Law, Antwerp/Oxford, Intersentia, 2006

Flaherty D. H., Protecting Privacy in Surveillance Societies (The University of North Carolina Press, 1989)

Gutwirth S., Leenes R., De Hert P., Poullet Y., European Data Protection: In Good Health? (Springer, 2012)

Gutwirth S., Poullet Y., De Hert P., Data Protection in a Profiled World (Springer, 2010)

Gutwirth S., Poullet Y., De Hert P., Leenes R., Computers, Privacy and Data Protection: an Element of Choice (Springer, 2011)

Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S., Reinventing Data Protection? (Springer, 2009)

Hildebrandt M., Gutwirth S., Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer, 2008)

Hondius F. W., Emerging Data Protection in Europe (North Holland Publishing Company, 1975)

Knight A., and Ruddock L., Advanced Research Methods in the Built Environment, Blackwell Publishing Ltd, 2008

Korff D., Data Protection Law in Practice in the European Union (Federation of European Direct and Interactive Marketing and The Direct Marketing Association, 2005)

Kuner, C., European Data Protection Law: Corporate Compliance and Regulation (Oxford University Press, 2nd ed., 2007),

Kranenborg, H. R., Access to Documents and Data Protection in the European Union – On the Public Nature of Personal Data, Kluwer, 2007

Lessig, L., Code version 2.0 (Basic Books, 2006)

Mayer-Schönberger, V., Delete: The Virtue of Forgetting in the Digital Age Princeton University Press, 2009

Mayer-Schonberger V. and Cukier, K., Big Data: A Revolution that will Transform How We Live, Work, and Think, First Mariner Books, 2014

Palfrey, J., and Gasser, U., Born Digital: Understanding the First Generation of Digital Natives, Basic Books, 2008

Solove D. J., Rotenberg, M., Schwartz, P. M., Information Privacy Law (Aspen Publishers, 2006)

Sykes C. J., The End of Privacy (St. Martin's Press, 1999)

Westin A. F., Privacy and Freedom (Colombia Law Review, 1967)

Westin A. F., Baker. M. A., Databanks in a Free Society: Computers, Record-Keeping and Privacy (Quadrangle Books, 1972)

Articles and Papers

Alpa, G., The Meaning of 'Natural Person' and the Impact of the Constitution for Europe on the Development of European Private Law, European Law Journal, Vol. 10, No. 6, November 2004

Baraliuc, I., Online Profiles After Death: Legal and Technological Aspects of Handling Personal Data, Tilburg Institute for Law, Technology and Society, 2010

Bergkamp, L., EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy, Computer Law and Security Report Vol. 18 No. 1, 2002

Bikker, J., Disaster Victim Identification in the Information Age: The Use of Personal Data, Post-Mortem Privacy and the Rights of the Victim's Relatives, Scripted, Vol. 10, Issue 1, 2013

Bollier, D., The Promise and Peril of Big Data, The Aspen Institute, 2010

Bollmer, G. D., Millions Now Living Will Never Die: Cultural Anxieties About the Afterlife of Information, The Information Society: An International Journal, 29:3, 2013

Bongers, L. M. H., Disclosure of Medical Data to Relatives after the Patient's Death: Recent Legal Developments with respect to Relatives' Entitlements in the Netherlands, European Journal of Health Law 18, 2011

Brubaker, J. R., Hayes, G. R., Dourish, P., Beyond the Grave: Facebook as a Site for the Expansion of Death and Mourning, The Information Society: An International Journal 29:3, 2013

Bygrave, L. A., The Place of Privacy in Data Protection Law, UNSW Law Journal, Vol. 24 no. 1, 2001

Cahn, N., Postmortem Life On-Line, The George Washington University Law School, Vol. 25, No. 4, 2011

Calvert, C., The Privacy of Death: An Emergent Jurisprudence and Legal Rebuke to Media Exploitation and a Voyeuristic Culture, Digital Commons at Loyola Marymount University and Loyola Law School, 2006

Carroll, B., Landry, K., Logging On and Letting out: Using Online Social Networks to Grieve and Mourn, Bulletin of Science Technology and Society 30:341, 2010

Cate, F. H., Cullen P. and Mayer-Schonberger, V., Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines (Oxford Internet Institute, University of Oxford, March 2014)

Choi, H. and Varian, H., Predicting the Present with Google Trends, The Economic Record, Vol. 88, Special Issue June 2012

Church, S. H., Digital Gravescapes: Digital Memorializing on Facebook, The Information Society: An International Journal 29:3, 2013

Coudert, F., Towards a New Generation of CCTV Networks: Erosion of Data Protection Safeguards?, Computer Law and Security Review, 25, 2009

Darrow, J. J., and Ferrera, G. R., Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?

De Hert, P., and Papakonstantinou, V., The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals, Computer Law and Security Review 28, 2012

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

Gantz, J., and Reinsel, D., The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, IDC iView, 2012

George, G., Haas M., and Pentland, A., Big Data and Management, Academy of Management Journal, April 2014

Goldschmidt, K., Thanatechnology: Eternal Digital Life After Death, Journal of Pediatric Nursing 28, 2013

Gonzalez Fuster, G., and Gutwirth, S., Opening Up Personal Data Protection: A Conceptual Controversy, Computer Law and Security Review 29, 2013

Graham, C., Gibbs, M., and Aceti, L., Introduction to the Special Issue on the Death, Afterlife, and Immortality of Bodies and Data, The Information Society: An International Journal 29:3, 2013

Hackett, C., and Connolly, U., Privacy from Birth to Death and Beyond: European and American Perspectives, ScriptEd, Vol. 10, Issue 1, April 2013

Hamill, D., The Privacy of Death on the Internet: A Legitimate Matter of Public Concern or Morbid Curiosity, Journal of Civil Rights and Economic Development, Vol. 25, 2011

Harbinja, E., Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could be the Potential Alternatives?, Scripted, Vol. 10 Issue 1, April 2013

Hering, A., Post-Mortem Relational Privacy: Expanding the Sphere of Personal Information Protected by Privacy Law, University of Florida, 2009

Herold, R., Is There Privacy Beyond Death?, CSI Alert, March 2005

Hicks, A., The Right to Publicity after Death: Postmortem Personality Rights in Washington in the Wake of Experience Hendrix v. HendrixLicensing.com, Seattle University Law Review, Vol. 36, 2012

Jerome, J. W., Buying and Selling Privacy: Big Data's Different Burdens and Benefits, Stanford Law Review, Vol. 66:47, 3rd September 2013

Koffeman, N. R., The Right to Personal Autonomy in the Case Law of The European Court of Human Rights, Leiden, 2010

Koops, B. J., Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to be Forgotten' in Big Data Practice (ScriptEd, 2011)

Kamer, M. H., Do Animals and Dead People have Legal Rights?, Canadian Journal of Law and Jurisprudence, Vol. XIV No. 1, 2001

Kuner, C, Cate, F. H., Millard, C. and Svantesson, D. J. B., The Challenge of 'Big Data' for Data Protection, International Data Privacy Law, 2012 Vol. 2 No. 2

Kutler, N., Protecting Your Online You: A New Approach to Handling Your Online Persona After Death, Berkely Technology Law Journal, Vol. 26 No. 4, 2011

Laas-Mikko, K. and Sutrop, M., How do Violations of Privacy and Moral Autonomy Threaten the Basis of our Democracy?, TRAMES: A Journal of the Humanities & Social Science, Vol. 16 Issue 4, 2012

Lenard, T. M. and Rubin, P. H., The Big Data Revolution: Privacy Considerations, December 2013

Lingel, J., The Digital Remains: Social Media and Practices of Online Grief, The Information Society, 2013

Maciel, C., Issues of the Social Web Interaction Project Faced with Afterlife Digital Legacy, Universidade Federa de Mato Grosso, Labaoratorio de Ambientes Virtuais Interativos, Instituto de Computacao, Cuiaba, MT – Brasil

Mantelero, A., Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behaviour, International Data Privacy Law, Vol. 3 No. 4, 2013

McDonald, A. M., and Cranor, L. F., The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society Vol. 4 No. 3, 2008

McCallig, D., Facebook After Death: An Evolving Policy in a Social Network, International Journal of Law and Information Technology, 2013

McCallig, D., Private but Eventually Public: Why Copyright in Unpublished Works Matters in the Digital Age, ScriptEd Vol. 10, Issue 1, April 2013

McCrudden, C., Human Dignity and Judicial Interpretation of Human Rights, The European Journal of International Law, Vol. 19 No. 4, 2008

Mommers, L., Het Binnenste Buiten: Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout Schmidt, Leiden University, 2010

Morenz-Harbinger, M. A., The Networking Dead: An Attempt to Define Statutory Third-Party Publicity Rights in Digital Estates, 2013

Peers, S., The Directive on Data Protection and Law Enforcement: A Missed Opportunity?, University of Essex, 2012

Polonetsky, J. and Tene, O., Privacy and Big Data: Making Ends Meet, Stanford Law Review, September 2013

Poullet, Y., Data Protection Legislation: What is at Stake for our Society and Democracy?, Computer Law and Security Review 25, 2009

Prins, C., When Personal Data, Behavior and Virtual Identities become a Commodity: Would a Property Rights Approach Matter?, ScriptEd, Vol. 3 Issue 4, 2006

Purtova, N., Property Rights in Personal Data: Learning from the American Discourse (Computer Law and Security Review, 2009)

Purtova, N., Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table…and back on again?, Computer Law and Security Review, December 2013

Raab. D. C., The Distribution of Privacy Risks: Who Needs Protection?, The Information Society: An International Journal 14:4, 1998

Rees, C., Tomorrow's Privacy: Personal Information as Property, International Data Privacy Law Vol. 3 No. 4, 2013

Richards N. M. and King, J. H., Three Paradoxes of Big Data, Stanford Law Review Vol. 66:41, 2013

Ringelheim, J., Processing Data on Racial or Ethnic Origin for Anti-Discrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?, Center for Human Rights and Global Justice Working Paper No. 13, 2006

Rosenblatt, A., International Forensic Investigations and the Human Rights of the Dead, Human Rights Quarterly, Vol. 32 No. 4, 2010

Rosler, H., Dignitarian Posthumous Personality Rights – An Analysis of U.S. and German Constitutional and Tort Law, Berkeley Journal of International Law, Vol. 26, Issue 1, 2008

Samuelson, P., Privacy as Intellectual Property (Stanford Law Review 52, 1999)

Schwartz, P. M., Property, Privacy and Personal Data, Harvard Law Review, Vol. 117 No 7, May 2004

Sherlock, A., Larger Than Life: Digital Resurrection and the Re-Enchantment of Society, The Information Society: An International Journal, 29:3, 2013

Sloot, B., Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation, International Data Privacy Law, 2014

Smolensky, K. R., Rights of the Dead, Hofstra Law Review, Vol. 37, 2009
Solove, D. J., "I've Got Nothing to Hide" and Other Misunderstandings of Privacy,

Solove, D. J., Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review Vol. 126, 2013

Suwala, A., Privacy of the Deceased: Posthumous Protection of Online Personae, University of Ottawa

Tasioulas, J., 'The Moral Reality of Human Rights' in Ethical and Human Rights Dimensions of Poverty: Towards a New Paradigm in the Fight against Poverty, Philosophy Seminar, UNESCO Poverty Project, All Souls College, Oxford, March 2003

Tasse, A., The Return of Results of Deceased Research Participants, Journal of Law, Medicine and Ethics, Winter 2011

Tene, O. and Polonetsky, J., Privacy in the Age of Big Data: A Time for Big Decisions, Stanford Law Review, February 2012

van Boom W. H. and Ogus, A., Introducing, Defining and Balancing 'Autonomy v. Paternalism', Erasmus Law Review, Vol. 3 Issue no. 2, 2010

Warren, S. D., and Brandeis, L. D., The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, 1890

Wilkens, M., Privacy and Security during Life, Access after Death: Are They Mutually Exclusive?, Hastings Law Journal, Vol. 62, March 2011

Online Articles, Papers and Blogs

How Amazon is Leveraging Big Data accessed via http://www.bigdata-startups.com/BigData-startup/amazon-leveraging-big-data/

How Big Data Enabled Spotify to Change the Music Industry accessed via http://www.bigdata-startups.com/BigData-startup/big-data-enabled-spotify-change-music-industry/

Ryanair and Google Set Out to Disrupt Travel Distribution, 14th January 2014 accessed via http://thinkdigital.travel/knowledgestream/ryanair-and-google-set-out-to-disrupt-travel-distribution/

Zynga is a Big Data Company Masqueraded as a Gaming Company accessed via http://www.bigdata-startups.com/BigData-startup/zynga-is-a-big-data-company-masqueraded-as-a-gaming-company/ on 20th July 2014

Anderson, N., Why Google Keeps Your Data Forever, Tracks You with Ads, 8th March 2010, accessed via http://arstechnica.com/tech-policy/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys/

Clark, J., Big Data or Big Data Hoarding?, 14th March 2013 accessed via http://www.datacenterjournal.com/it/big-data-big-data-hoarding/

Drew, S., Big Data Hoarding can be a Big Problem, 11th July 2014 accessed via http://midsizeinsider.com/en-us/article/big-data-hoarding-can-be-a-big-problem

Edwards L. and Harbinja, E., What Happens to my Facebook Profile when I Die?: Legal Issues around Transmission of Digital Assets on Death, 21st February 2013 accessed via http://ssrn.com/abstract=2222163

Herold, R., 10 Big Data Analytics Privacy Problems, 30th June 2014 accessed via http://midsizeinsider.com/en-us/article/10-big-data-analytics-privacy-problems on 23rd July 2014

Hilderbrandt, M., Slaves to Big Data. Or Are We?, Selected Works of Mireille Hildebrandt accessed via http://works.bepress.com/mireille_hildebrandt/52

Hopkins, R., The Day I Closed My Amazon Account, 5th December 2013 accessed via https://www.transitionnetwork.org/blogs/rob-hopkins/2013-12/day-i-closed-my-amazon-account on 20th July 2014

Hutchins, R., Perspective: Looking Forward to Life with Big Data, 2nd January 2014 accessed via http://emcien.com/perspective-looking-forward-life-big-data/

Hutchinson T., and Duncan, N., Defining What We Do – Doctrinal Legal Research accessed via http://www.scribd.com/doc/191621387/Hitchinson-and-Duncan

Leonard, A., How Netflix is Turning Viewers into Puppets, Salon, 1st February 2013

Marr, B., Big Data: The Mega-Trend That Will Impact All Our Lives, 27th August 2013 accessed via https://www.linkedin.com/today/post/article/20130827231108-64875646-big-data-the-mega-trend-that-will-impact-all-our-lives

Marr, B., Facebook's Big Data: Equal Parts Exciting and Terrifying?, 18th February 2014 accessed via http://smartdatacollective.com/bernardmarr/185086/facebook-s-big-data-equal-parts-exciting-and-terrifying on 23rd July 2014

McCallig, D., The Law of Digital Remains, accessed via http://research.ie/intro_slide/law-digital-remains

Nemschoff, M., 7 Important Types of Big Data, Smart Data Collective, 2014 accessed via http://smartdatacollective.com/michelenemschoff/187751/7-important-types-big-data/

O' Loughlin, E., The Ryanair and Google Partnership – What's In It For Us?, 31st January 2014 accessed via http://businessetc.thejournal.ie/readme/ryanair-and-google-partnership-%E2%80%93-what%E2%80%99s-in-it-for-us-1291150-Jan2014/ on 20th July 2014

Passingham, M., eBay Using Big Data Analytics to Drive Up Price Listings, 22nd October 2013 accessed via http://www.v3.co.uk/v3-uk/news/2302017/ebay-using-big-data-analytics-to-drive-up-price-listings on 20th July 2014

Saran, C., Case Study: How Big Data Powers the EBay Customer Journey, 29th April 2014 accessed via http://www.computerweekly.com/news/2240219736/Case-Study-How-big-data-powers-the-eBay-customer-journey on 20th July 2014

UN Global Pulse, Big Data for Development: Challenges & Opportunities, May 2012 accessed via http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf

Wu, L. and Brynjolffson, E., The Future of Prediction: How Google Searches Foreshadow Housing Prices and Sales, draft of May 2014 accessed via http://www.nber.org/chapters/c12994.pdf

Other Online Materials

Amazon Conditions of Use and Sale accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=1040616

Amazon Help Page, Edit Your Profile, accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=help_search_1-7?ie=UTF8&nodeId=200039420&qid=1405938238&sr=1-7

Amazon Help Page, Manage Your Browsing History accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=help_search_1-1?ie=UTF8&nodeId=15891461&qid=1405938359&sr=1-1

Amazon.co.uk Privacy Notice accessed via http://www.amazon.co.uk/gp/help/customer/display.html/ref=gss?nodeId=502584

Dropbox Help Centre, Can I access the Dropbox account of someone who has passed away?, accessed via https://www.dropbox.com/help/488/en

eBay Privacy Notice accessed via http://pages.ebay.co.uk/help/policies/privacy-policy.html?rt=nc

Facebook Data Use Policy accessed via https://www.facebook.com/about/privacy/your-info

Facebook FAQs, What happens to content (posts, pictures) that I delete from Facebook?, accessed via https://www.facebook.com/help/356107851084108

Facebook Application Forms, Special Request for Deceased Person's Account, accessed via https://www.facebook.com/help/contact/228813257197480

Facebook FAQs, How do I submit a special request for a deceased user's account on the site? Accessed via https://www.facebook.com/help/www/265593773453448

Gmail Account Access Issues, Accessing a deceased user's mail, accessed via https://support.google.com/mail/answer/14300?hl=en

Google Help Page, About Inactive Account Manager, accessed via https://support.google.com/accounts/answer/3036546?hl=en

Google Public Policy Blog, Plan your digital afterlife with Inactive Account Manager, accessed via http://googlepublicpolicy.blogspot.nl/2013/04/plan-your-digital-afterlife-with.html

Google Privacy Policy, accessed via https://www.google.com.mt/policies/privacy/#infouse

Ryanair Website Privacy Statement accessed via http://www.ryanair.com/mt/privacy-policy/

Spotify Privacy Policy accessed via https://www.spotify.com/uk/legal/privacy-policy/#information

Zynga Privacy Policy accessed via https://company.zynga.com/privacy/policy

Opinions

Article 29 Data Protection Working Party 00569/13/EN WP 203, Opinion 03/2013 on purpose limitation adopted on 2 April 2013

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20th June 2007.

Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN WP 105, 19th January 2005

Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014 accessed via https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf on 28th June 2014.

Lectures and Presentations

Ambrose, M., Where has the Time Gone? An Information Life Cycle Approach to the Right to be Forgotten, in Computers, Privacy and Data Protection Conference, Brussels, 23rd January 2014

Korenhof, 'Timing the Right to be Forgotten', delivered at the Computers, Privacy and Data Protection Conference on 23rd January 2014 accessed via http://www.cpdpconferences.org/Resources/23_GH_1030_KORENHOF.pdf

McCallig, D., 'Post-Mortem Privacy: Exploring Deceased's Privacy in a Digital World', in Computers, Privacy and Data Protection Conference, Brussels, 24th January 2014

Moerel, L., Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof, Lecture delivered during the public acceptance of the appointment of professor of Global ICT Law at Tilburg University, 14th February 2014

Other Materials

Centre for Information Policy Leadership, Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance, Discussion Document, Hunton & Williams LLP, February 2013

European Commission Factsheet, Why do we need an EU data protection reform?, accessed via http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf on 18th June 2014

Press Release on the 3319th Council meeting, Justice and Home Affairs, Luxembourg, 5th and 6th June 2014 accessed via http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/143119.pdf

Roagana, I., 'Protecting the right to respect for private and family life under the European Convention on Human Rights' in Council of Europe Human Rights Handbooks, Strasbourg, 2012

World Economic Forum, Personal Data: The Emergence of a New Asset Class, 2011

World Economic Forum, Rethinking Personal Data: A New Lens for Strengthening Trust, May 2014

Legislation and Related Texts

European Legislation

Charter of Fundamental Rights of the European Union (2000/C 364/01), 18th December 2000

Convention for the Protection of Human Rights and Fundamental Freedoms, 4th November 1950

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28th January 1981.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Commission Memo, LIBE Committee votes back new EU data protection rules, Brussels, 22nd October 2013

European Commission Memo, Progress on EU data protection reform now irreversible following European Parliament vote, Strasbourg, 12th March 2014

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) accessed via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20140312+ITEMS+DOC+XML+V0//EN&language=EN#top

Inofficial Consolidated Version after LIBE Committee Vote provided by the Rapporteur, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 22nd October 2013

Note from the Presidency to the Working Party on Data Protection and Exchange of Information, on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of data and on the free movement of such data (General Data Protection Regulation) 22nd June 2012

Note from the Presidency to the Working Party on Information Exchange and Data Protection on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of data and on the free movement of such data (General Data Protection Regulation), 16th December 2013

Note from the Presidency to the Council on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter V, 28th May 2014

Note from the Presidency to the Working Party on Information Exchange and Data Protection on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of data and on the free movement of such data (General Data Protection Regulation), 30th June 2014

National Legislation

23750 Organic Law 15/1999 of 13 December on the Protection of Personal Data, Spain

Act on Protection of Personal Data (Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll.), Slovakia

The Act on Processing of Personal Data (Act No. 429 of 31 May 2000 as amended by section 7 of Act No. 280 of 25 April 2001, section 6 of Act No. 552 of 24 June 2005 and section 2 of Act No. 519 of 6 June 2007), Denmark

Data Protection Act, 16th July 1998, The United Kingdom

Data Protection Act, 15th July 2003 (Chapter 440 of the Laws of Malta)

Loi Informatique Et Libertes Act N°78-17 Of 6 January 1978 On Information Technology, Data Files And Civil Liberties amended by the following laws: Act Of 6 August 2004 Relative To The Protection Of Individuals With Regard To The Processing Of Personal Data Act Of 13 May 2009 Relative To The Simplification And Clarification Of Law And Lighter Procedures Law No.2009-526 Dated 13/05/2009 Organic Law No.2010-704 Dated 28/06/2010 Law No.2011-334 Dated 29 March 2011 Relative To The Défenseur Des Droits Ordinance No.2011-1012 Dated 24/08/2011

Personal Data Act (1998: 204), Sweden, 29th April 1998

Personal Data Protection Act (Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts), Czech Republic

Personal Data Protection Act of the Republic Of Slovenia (No. 001-22-148/04), 15th July 2004

Personal Data Protection Act Promulgated State Gazette No. 1/4.01.2002, effective 1.01.2002, supplemented, SG No. 70/10.08.2004, effective 1.01.2005, SG No. 93/19.10.2004, No. 43/20.05.2005, effective 1.09.2005, amended and supplemented, SG No. 103/23.12.2005, amended, SG No. 30/11.04.2006, effective 12.07.2006, Bulgaria

Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003, Italy

Republic of Lithuania Law on Legal Protection of Personal Data (21 January 2003, No. IX-1296)

Case Law

European Court of Human Rights

Amann v. Switzerland, Application No. 27798/95, 16th February 2000

Akpinar and Altun v. Turkey, App No 56760/00, 27th February 2007

Gaskin v. The United Kingdom, App No 10454/83, 7th July 1989

Jaggi v. Switzerland, App No. 58757/00, 13th October 2006

Leander v. Sweden App No 9248/81, 26th March 1987

Odievre v France, App. No. 42326/98, 13th February 2003

Pannullo and Forte v. France, App No 37794/97, 2001

Pretty v. The United Kingdom, App No 2346/02, 2002

Rotaru v. Romania App No. 28341/95, 4th May 2000

The Estate of Kresten Filtenborg Mortensen v. Denmark, App No 1338/03, 15th May 2006

Znamenskaya v. Russia, App No 77785/01, 2005

European Court of Justice

Case C-101/01, Criminal Proceedings against Lindqvist, 6th November 2003

Joint cases C-465/00 and C-138/1Rechnungshof v. Osterreichischer Rundunk and Others, 20th May 2003

National Courts

Mephisto, Bundesverfassungsgericht [BVerfG], German Federal Constitutional Court, 1971.

Websites

http://www.amazon.co.uk/

http://www.bigdata-startups.com/

https://www.bookryanair.com/

http://www.bloomberg.com

http://www.dropbox.com/

http://www.ebay.co.uk/

http://www.echr.coe.int/

http://www.europa.eu/

http://www.europarl.europa.eu/

http://www.facebook.com./

http://www.gooogle.com/

https://www.google.com/flights/

http://www.google.com/trends/

http://hudoc.echr.coe.int/

http://www.ryanair.com/

http://www.spotify.com/

http://www.twitter.com/

http://www.zynga.com/