**11. The Digital Afterlife**

‘Digital afterlife’ refers to a continuation of an active or passive digital presence after a person’s death. It is a virtual space where information, assets, legacies, and digital remains reside as part of the cyber soul.[[1]](#footnote-1) Digital remains are “the digital content and data which was accumulated and stored online during our lifetime that reflect our digital personality and memories.”[[2]](#footnote-2) When internet users pass away, their digital remains may still be used by the living. For instance, the living may communicate to chatbots and avatars created by artificial intelligence (AI) that adopt characteristics of the deceased based on algorithms, and an executor of a deceased estate may deal with digital assets and social media accounts can be ‘memorialised’.

Ethical concerns have been raised about having individuals immortalised in the digital space, however, discourse regarding the legal implications of this emerging issue has remained limited.

1. **AI and the Digital Afterlife Industry**

The internet has become a space where the dead and the living co-inhabit. The number of dead accounts online is expected to surpass the living population by the end of this century.[[3]](#footnote-3) Projects including [LifeNaut](https://www.lifenaut.com/), [Eternime](https://eternime.breezy.hr/), [Replika](https://replika.com/), [Project December](https://projectdecember.net/) powered by OpenAI, and [ETER9](https://www.eter9.com/) have emerged to take advantage of the new Digital Afterlife Industry (**DAI**). These social networks utilise AI machine-learning technology, which allows the AI to recognise patterns in user behaviour and data to digitally replicate the deceased. DAI is defined as an umbrella term encompassing “any activity of production of commercial goods (or services) that involves online usage of digital remains”. An example is two-way communication with AI[[4]](#footnote-4) chatbots and avatars impersonating the deceased (also known as ‘griefbots’ or ‘deadbots’).[[5]](#footnote-5) For example, the AI in ETER9 creates a virtual counterpart to users (known as ‘Niners’) that learn and mimics the users’ online behaviour. These counterparts can interact online autonomously, i.e. post, comment and ‘like’, whilst assuming the user’s personality and characteristics, even after the biological user has passed. Some people communicate with these deceased’s counterparts to process grief.[[6]](#footnote-6) However, once users of these projects die, they no longer have control over their data and posthumous self, which has been permanently left on the internet to be consumed by the algorithm.

1. **Post-mortem privacy protection**

Issues that arise are the current lack of regulation for DAI companies such as ETER9 and the concern for an individual’s posthumous privacy protection. The notion of ‘post-mortem privacy’ (**PMP**), suggests that privacy, personal data and testamentary freedom forms part of a person’s autonomy and should be respected the same way as a physical body.[[7]](#footnote-7) PMP has been conceptualised as ‘the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memories after death’.[[8]](#footnote-8) PMP emphasises the importance of a person’s control over their data after death. However, the right to privacy does not typically apply to deceased persons.

The [*General Data Protection Regulation*](https://gdpr-info.eu/) (**GDPR**), introduced in 2014 by the European Union, provides the right to be forgotten online with the aim of “protect[ing] fundamental rights and freedoms of *natural persons* and in particular their right to the protection of personal data”.[[9]](#footnote-9) ‘Natural persons’ does not include dead persons. Similarly, the Australian *Privacy Act 1988* (Cth)does not extend the right to be forgotten to the deceased. However, there have been some instances where the possibility of providing privacy protection to the deceased has been shown. Section 9 of the *Personal Data Protection Act 2018* of Estonia provides that the consent of processing personal data is “valid during the lifetime of the data subject and for 10 years after the death of the subject matter.” This approach may be considered by common law countries in the future.

Allowing AI to utilise the digital remains of deceased people might also be considered a violation of their dignity.[[10]](#footnote-10) However, the protection of an individual’s dignity is currently only recognised in common law (i.e. against defamation) and does not extend post-mortem.

While, PMP is currently not recognised under succession laws or privacy, an individual could clarify their intentions of their digital assets by way of social media providers’ online tools (eg social media legacy contacts or similar) or testamentary dispositions.

1. **Social media**

Social media platforms are also part of the DAI, with some allowing inactive profiles to remain as a place of remembrance for the deceased. This has been described as ‘online cemeteries’. [[11]](#footnote-11) In 2009, Facebook introduced a [legacy contact function](https://www.facebook.com/help/1568013990080948), which allows users to appoint a person to manage their memorialised main profile or have their account permanently deleted. The legacy contact may post a final message, respond to friend requests, and update the profile photo; however, they are unable to access the account and the user’s private messages. Accounts on [Instagram](https://help.instagram.com/231764660354188?helpref=faq_content) may also be memorialised, with the word ‘Remembering’ appearing next to the deceased’s profile name. People can also appoint an ‘[Inactive Account Manager](https://support.google.com/accounts/answer/3036546?hl=en)’ for their Google account.

1. **Digital assets and the law**

Digital assets are described as ‘any digital file on a person’s electronic device as well as any online accounts and memberships’. These assets include (but are not limited to) email accounts, social media accounts, digital photos, digital videos, cryptocurrency and online subscription accounts. Digital assets, to be identified clearly, can be categorised into different kinds of value. Nonetheless, the asset can be categorised into more than one value.

Digital assets can have financial, sentimental, social and intellectual value.[[12]](#footnote-12) Digital assets with financial value include bank accounts and cryptocurrency. These assets have a definite monetary value. Digital assets with sentimental value do not have monetary value, but rather sentimental in nature such as photographs and videos. Digital assets with social value include social media platforms where users have curated their accounts which allows them to connect with new people and portray their lives. Digital assets with intellectual value include emails, blogs, social media posts (written and visual material) that is published material. However, an asset with intellectual value may become a liability if the published material is defamatory to another individual. A deceased person cannot be sued; however, an estate of a deceased person can be sued if their published material is libel.

Currently, there is a lack of guidelines in Australia for how someone can access a deceased’s digital assets. The United States introduced the *Revised Uniform Fiduciary Access to Digital Assets Act 2015[[13]](#footnote-13)* and Canada enacted a similar legislation in 2016 called the *Uniform Access to Digital Assets by Fiduciaries Act.[[14]](#footnote-14)* These laws authorise a representative to access digital assets if that power was expressed in the deceased’s willor other legal document such as a power of attorney. In 2022, the Australian Attorney-General’s Department released the *Privacy Act Review Report[[15]](#footnote-15)* endorsing the introduction of an access scheme for digital records. The Australian Government is yet to implement the recommendations in this report.

1. **Digital assets and succession**

In Australia, there are no laws that require testamentary acts to include digital assets, such as what directions the executor is given to either continue or delete social media profiles, online subscriptions or emails. It is up to the discretion of solicitors to raise what digital assets the testator owns as well as discussing with the client that they should provide their executor with their passwords upon their death to allow the executor to access and close or manage accounts. The NSW Law Reform Commission (**‘NSWLRC’**) published a report ‘Access to Digital Records Upon Death or Incapacity’ in 2019 that thoroughly discussed amendments that need to be made to the current succession laws and estate laws to reflect digital assets, and to provide education to legal practitioners to assist clients in their decision-making when preparing their testamentary dispositions and providing their directions to their executor/s, trustees, guardians and attorneys.[[16]](#footnote-16)

The NSWLRC conducted two surveys to understand how digital assets should be dealt with upon death or incapacity. The first survey was asking the public “what should happen to your social media when you die?”, and the second survey was asking legal practitioners 43 questions ranging from “do you practice estate planning” and “is advising personal representatives about administering deceased estates part of your practice?”. The results concluded that not many people have thought about their digital assets.

The results can be found [here](https://lawreform.nsw.gov.au/documents/Publications/Other-Publications/Research-Reports/RR15.pdf).

1. Maggi Savin-Baden and Victoria Mason-Robbie, Digital Afterlife: *Death Matters in a Digital Age (CRC Press LLC, 2020)*, 12-3. [↑](#footnote-ref-1)
2. Maggi Savin-Baden and Victoria Mason-Robbie (ed), *Digital Afterlife: Death Matters in a Digital Age* (CRC Press LLC, 2020), 13. [↑](#footnote-ref-2)
3. Ibid, 139. [↑](#footnote-ref-3)
4. Tal Morse, ‘Digital necromancy: users’ perceptions of digital afterlife and posthumous communication technologies.’ (2024) 27(2) *Information, communication & society*, 240, 245. [↑](#footnote-ref-4)
5. Tomasz Hollanek and Katarzyna Nowaczyk-Basińska, ‘Griefbots, Deadbots, Postmortem Avatars: On Responsible Applications of Generative AI in the Digital Afterlife Industry’ (2024) 37(2) *Philosophy & Technology*, 63, 63. [↑](#footnote-ref-5)
6. Belén Jiménez-Alonso and Ignacio Brescó de Luna, ‘Griefbots. A New Way of Communicating With The Dead?’ *Integrative Physiological and Behavioral Science*, (2023) 57(2), 466. [↑](#footnote-ref-6)
7. Edina Harbinja, *Digital Death, Digital Assets and Post-Mortem Privacy* (Edinburgh University Press, 2022), 54. [↑](#footnote-ref-7)
8. Ibid. [↑](#footnote-ref-8)
9. *General Data Protection Regulation* (EU) 2016/679, [2016] OJ L119/1, art 1 (emphasis added). [↑](#footnote-ref-9)
10. Carl Öhman and Luciano Floridi, ‘The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry’ (2017) 27(4), *Minds and Machines (Dordrecht),* 639, 639. [↑](#footnote-ref-10)
11. Chloe Cooper, ‘Mourning the dead in the digital afterlife’ (2020) *Kill Your Darlings New Fiction, Essays, Commentary and Reviews* 136, 137. [↑](#footnote-ref-11)
12. Ibid 131-2. [↑](#footnote-ref-12)
13. *Revised Uniform Fiduciary Access to Digital Assets Act* (2015) (Uniform Law Commission). [↑](#footnote-ref-13)
14. *Uniform Access to Digital Assets by Fiduciaries Act* (2020) (Uniform Law Conference of Canada). [↑](#footnote-ref-14)
15. Attorney-General’s Department (Commonwealth), *Privacy Act Review Report 2022* (2022). [↑](#footnote-ref-15)
16. New South Wales Law Reform Commission, *Access to digital records upon death or incapacity* (Report No 147, December 2019), xvii. [↑](#footnote-ref-16)