Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Governing ghostbots

Edina Harbinja[a,*], *Lilian Edwards*[b], *Marisa McVey*[c]

[a] *Aston Law School, Aston University, UK*
[b] *Newcastle Law School, Newcastle University, UK*
[c] *School of Law, Queen's University Belfast, UK*

ARTICLE INFO

Keywords:
Ghostbots
Deepfakes
Post-mortem privacy
Digital legacy
Digital remains

ABSTRACT

This article discusses the legal implications of a novel phenomenon, namely, digital reincarnations of deceased persons, sometimes known as post-mortem avatars, deepfakes, replicas, holographs, or chatbots. To elide these multiple names, we use the term 'ghostbots'. The piece is an early attempt to discuss the potential social and individual harms, roughly grouped around notions of privacy (including post-mortem privacy), property, personal data and reputation, arising from ghostbots, how they are regulated and whether they need to be adequately regulated further. For reasons of space and focus, the article does not deal with copyright implications, fraud, consumer protection, tort, product liability, and pornography laws, including the non-consensual use of intimate images ('revenge porn'). This paper focuses on law, although we fully acknowledge and refer to the role of philosophy and ethics in this domain.

We canvas two interesting legal developments with implications for ghostbots, namely, the proposed EU Artificial Intelligence (AI) Act and the 2021 New York law amending publicity rights to protect the rights of celebrities whose personality is used in post-mortem 'replicas'. The latter especially evidences a remarkable shift from the norm we have chronicled in previous articles of no respect for post-mortem privacy to a growing recognition that personality rights do need protection post-mortem in a world where pop stars and actors are routinely re-created using AI. While the legislative motivation here may still be primarily to protect economic interests, we argue it also shows a concern for dignitary and privacy interests.

Given the apparent concern for the appropriation of personality post-mortem, possibly in defiance or ignorance of what the deceased would have wished, we propose an early solution to regulate the rise of ghostbots, namely an enforceable 'do not bot me' clause in analogue or digital wills.

1. Introduction

In February 2021, the genealogy site MyHeritage released their new service called 'DeepNostalgia', allowing users to animate

* Corresponding author.
E-mail address: e.harbinja@aston.ac.uk (E. Harbinja).

https://doi.org/10.1016/j.clsr.2023.105791

still photographs of late relatives and share these across various platforms.[1] The service uses technology licensed from a deep-learning start-up company called D-ID,[2] which enables 'video re-enactment': fixed sequences of movements and gestures are applied to uploaded still photos, allowing the photos' inhabitants to smile and blink.[3] According to the MyHeritage website, there have been 78 million photo animations since the launch of DeepNostalgia, which flooded social media platforms around the time of release.[4]

MyHeritage is just one of emerging genres of services or products that attempt to replicate the appearance, voice and/or personality of a deceased person after their death, primarily using machine learning techniques commonly termed 'AI', though some are simple rule-based systems. They are a subset of the increasingly well-known phenomenon of 'deepfakes', a word which is a portmanteau of both 'deep learning' and 'fake'.[5] 'Deepfakes' is a term typically used to refer to an image or video of someone that has been created, altered or manipulated using artificial intelligence (AI) in a way that makes the fabricated media look authentic. The definition of deepfake is amorphous and expanding, covering various applications – including face and body-swapping, morphing or full-body puppetry, audio-swapping, and lip-synching.[6] Deepfakes have usually relied on training generative neural network architectures, where a target's information can be superimposed on an original photo or video to alter it.[7] Other machine learning techniques, such as 'generative adversarial networks' (GANs),[8] can be applied to ensure the image or video constantly evolves and improves, creating even more convincing synthesised media. Most recently, extremely convincing deepfake or generative images have been produced using diffusion algorithms, which have founded extremely popular AI-generated art models such as Stable Diffusion, MidJourney and DALL-E 2.[9] These sites generate images from a natural language text prompt, do not require programming of any kind and are available either free or for a relatively small fee. They have been the popular success story of 2022, with tens of millions of users amassed in very short order. Some models, such as Stable Diffusion, have furthermore been released as 'open source', meaning that users can adapt them as they please for both positive and disturbing or 'not safe for work' (NSFW) purposes. These developments will inevitably percolate into the production of ghostbots.

MyHeritage is an outstanding, though by no means sole, example of what in this article we will term *ghostbots*, i.e. digital reincarnations of deceased persons, usually though not exclusively created using AI techniques, sometimes also known as post-mortem avatars, deepfakes, replicas, holographs, or chatbots. This piece is an early attempt to discuss the potential social and individual harms, roughly grouped around notions of privacy (including post-mortem privacy), property, personal data and reputation, arising from ghostbots, how they are regulated and whether they need to be adequately regulated further. For reasons of space and focus, the article does not deal more than passingly with copyright implications, fraud, consumer protection, tort, product liability, and pornography laws, including non-consensual use of intimate images ('revenge porn'). This paper is written by legal academics and focuses on law, although we fully acknowledge the role of philosophy and ethics in this domain.[10]

[1] MyHeritage website < https://www.myheritage.com/deep-nostalgia> accessed 20 February 2022.

[2] D-ID website < https://www.d-id.com/> accessed 20 February 2022.

[3] My Heritage, 'Deep Nostalgia FAQs' <https://www.myheritage.com/deep-nostalgia> accessed 20 February 2022.

[4] Eric Krebs, 'Is Animating Dead Relatives with AI Cathartic or Creepy? Yes. *VICE* (17 March 2021), <https://www.vice.com/en/article/z3vaq8/is-animating-dead-relatives-with-ai-cathartic-or-creepy-yes> accessed 20 February 2022.

[5] Yisroel Mirksy and Wenke Lee, 'The Creation and Detection of Deepfakes: A Survey', (2020) 54(1) *ACM Computing Surveys*, 1.

[6] Dolhansky et al, 'The Deepfake Detection Challenge (DFDC) Preview Dataset', (2019) *Computer Science*

[7] See: Bobby Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', (2019) 107 *California Law Review,* 1753; Yisroel Mirksy and Wenke Lee, 'The Creation and Detection of Deepfakes: A Survey', (2020) 54(1) *ACM Computing Surveys*, 1.

[8] GANs brings two neural networks to compete against each other; one creates fake samples with the aim of fooling the other into determining that the generated content is real and not computer-generated. As this process continues, the neural network generating the fake samples learns to create content that is indistinguishable from real content. When this technology is applied in the context of deepfakes, it creates images or videos that are seem authentic. See: Ian J. Goodfellow et al., 'Generative Adversarial Nets' (Neural Information Processing Systems Conference, 10 June 2014).

[9] See https://stability.ai/blog/stable-diffusion-public-release, https://www.midjourney.com/ and https://openai.com/dall-e-2/, all accessed 22 December 2022. Although all these sites currently generate still images, text-to-video models are also emerging slowly into the consumer market. Interestingly both Stable Diffusion and DALL-E 2 originally banned the use of real person images in their systems, primarily to prevent revenge porn and blackmail uses; however, both have relaxed this prohibition subsequently under public demand. Tools are emerging for data subjects to track down and refuse use of their image eg Source+, a standard aiming to allow people to disallow their work or likeness to be used for AI training purposes, but none are mandatory or widely known. See Kyle Wiggers 'OpenAI removes the waitlist for DALL-E 2, allowing anyone to sign up', (*Techcrunch*, September 28, 2022) <https://techcrunch.com/2022/09/28/openai-removes-the-waitlist-for-dall-e-2-allowing-anyone-to-sign-up/> accessed 22 December 2022.

[10] See for example Fiorenza Gamba, 'AI, mourning and digital immortality. Some ethical questions on digital remain and post-mortem privacy' 157 (2022) *Études sur la mort*, 157, 13-25. https://doi.org/10.3917/eslm.157.0013; Alexis Elder, 'Conversations From Beyond the Grave? A Neo-Confucian Ethics of Chatbots of the Dead' 37(1) (2020) *J Applied Philos*, 73-88; Belén Jiménez-Alonso, B., & Ignacio Brescó de Luna, 'Griefbots. A New Way of Communicating With The Dead?' (2022) *Integrative psychological & behavioral science*. doi:10.1007/s12124-022-09679-3; Maggi Savin-Baden, 'The ethics and impact of digital immortality' 02 (2017) *Knowledge Cultures*, 178-196; Davide Sisto, *Online Afterlives: Immortality, Memory, and Grief in Digital Culture* (2020, MIT Press), Carla Sofka, 'The transition from life to the digital afterlife. Thanatechnology and its impact on grief' In M. Savin-Baden & V. Mason-Robbie (Eds.), *Digital afterlife. Death Matters in a Digital Age* (2020, New York: Chapman and Hall/CRC); Patrick Stokes, *Digital souls: a philosophy of online death* (2021, London: Bloomsbury Academic).

2. Deepfakes and ghostbots

2.1. *Deepfakes of the living*

This article focuses on the issues of recreating the personality or appearance of humans after their death, but it is useful to situate this in the general explosion in creativity and technique in building replicas of the living. Famous examples of 'living' deepfakes include the viral impersonation of actor Tom Cruise on TikTok ;[11] the TikTok account jojobiden46 that gained 1.2 million followers during the US election ;[12] and Buzzfeed's Barack Obama deepfake, where the former president speaks of the dangers of this new technology.[13] Although all these were produced primarily for entertainment or advertising value, deepfakes have also been utilised for more sinister purposes. Most notoriously, deep fakes are frequently used for non-consensual image-based sexual abuse or fake pornography,[14] generated to humiliate, harm, or seek financial gain.[15] Deepfakes have been a destabilising influence in politics,[16] spreading disinformation[17] and enabling criminal activity.[18]

While manipulation of images, audio or video is certainly not a new phenomenon, the increasing sophistication of machine learning is generating more believable synthesised media, and the democratisation of this technology – with free software downloads, YouTube tutorials, and social media filters – allows for greater diffusion and accessibility.[19] This has resulted in a situation wherein 'technologically unsophisticated actors are now able to create a wide array of deep fakes' and share this across a multitude of online platforms.[20]

2.2. *Deepfakes of the dead: the rise of ghostbots*

We turn now to the use of deepfakes in the context of the deceased, or 'ghostbots'. As previously analysed by Edwards and Harbinja, ghostbots are no longer purely within the realm of science fiction.[21] Holographing the dead is becoming nostalgia-based 'big business',[22] with Kanye West making headlines in 2020 with his birthday present to Kim Kardashian – a holograph of her late father, Robert Kardashian – using deepfake technology.[23] While post-mortem revival of celebrities is potentially profitable, it was reported in *Wired* in 2018 that the companies bringing famous names such as Tupac Shakur and Michael Jackson back to life remain mired in a state of 'near-constant litigation', either with the deceased's estate or rival holograph companies.[24] Deepfake technology may be used to recreate post-mortem voices as well as images, as seen in a documentary about deceased TV chef Antony Bourdain was added saying words he never recorded while alive.[25] The film director clashed with Bourdain's wife, the lit-

[11] Mitchell Clarke 'This TikTok Tom Cruise Impersonator is Using Deepfake Technology to Impressive Ends', *The Verge* (26 February 2021) <https://www.theverge.com/22303756/tiktok-tom-cruise-impersonator-deepfake> accessed 20 February 2022.

[12] TikTok, JoJoBiden46 account, https://www.tiktok.com/@jojobiden46/video/6888445134149668101 accessed 20 February 2022.

[13] BuzzFeed Video, 'You won't Believe What Obama Says in This Video!' (17 April 2018) <https://www.youtube.com/watch?v=cQ54GDm1eL0&ab_channel=BuzzFeedVideo> accessed 20 February 2022.

[14] See: Russell Spivak, '"Deepfakes": The Newest Way to Commit one of the Oldest Crimes' (2019) 185(3) *Georgetown Law Technology Review,* 339; Douglas Harris, 'Deepfakes: False Pornography is Here and The Law Cannot Protect You', (2019) 17(1) *Duke Law & Technology Review,* 99; Henry Adjer, Giorgio Patrini and Francesco Cavalli, 'Automating Image Abuse: Deepfake Bots on Telegram' *Sensity* (October 2020) < https://www.medianama.com/wp-content/uploads/Sensity-AutomatingImageAbuse.pdf> accessed 20 February 2022.

[15] Chesney and Citron (n 7).

[16] See: Ali Breland, 'The Bizarre and Terrifying Case of the "Deepfake" Video that Helped Bring an African Nation to the Brink', *Mother Jones* (5 March 2019) < https://www.motherjones.com/politics/2019/03/deepfake-gabon-ali-bongo/> accessed 20 February 2022; Nilesh Christopher, 'We've Just Seen the First Use of Deepfakes in an Indian Election Campaign', *VICE* (18 February 2020) <https://www.vice.com/en/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp> accessed 20 February 2022; Nicholas Diakopoulas and Deborah Johnson, 'Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections', (forthcoming) *New Media and Society* <https://journals.sagepub.com/doi/pdf/10.1177/1461444820925811> accessed 20 February 2022.

[17] See: Brundage et al., 'Malicious Use of AI' (2018) <https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217> accessed 20 February 2022; James Vincent, 'Deepfake Satellite imagery Poses a Not-So-Distant Threat, Warn Geographers', *The Verge* (27 April 201) <https://www.theverge.com/2021/4/27/22403741/deepfake-geography-satellite-imagery-ai-generated-fakes-threat> accessed 20 February 2022.

[18] BBC News, 'Fake Voices 'Help Cyber-Crooks Steal Cash', (8 July 2019) <https://www.bbc.co.uk/news/technology-48908736> accessed 20 February 2022.

[19] See: Chesney and Citron (n 7); Karen Hao and Will Douglas Haven, 'The Year Deepfakes Went Mainstream', *MIT Technology Review* (24 December 2020) <https://www.technologyreview.com/2020/12/24/1015380/best-ai-deepfakes-of-2020> accessed 20 February 2022; Kelsey Farish, 'Personality Rights: From Hollywood to Deepfakes' in European Audiovisual Observatory (eds) *Artificial Intelligence In the Audiovisual Sector* (European Audiovisual Observatory 2020).

[20] Edvinas Meskys et al, 'Regulating Deep Fakes: Legal and Ethical Considerations', (2020) 15(1) *Journal of Intellectual Property Law & Practice,* 24, 25.

[21] Lilian Edwards and Edina Harbinja, '"Be Right Back": What Rights Do We Have Over Post-Mortem Avatars of Ourselves?' in Lilian Edwards, Edina Harbinja and Burkhard Schafer (eds), *Future Law, Emerging Technology, Regulation and Ethics* (Edinburgh University Press 2020). A recent stunning fictional exploration of near future deepfake technology used by police to bring to justice culprits whose criminal or terrorist acts were known but never recorded in real life, can be seen in the BBC's *The Capture* (2019, 2022)

[22] Jimi Famurewa, 'Inside the Bitter War to Bring Tupac and Michael Jackson Back to Life', *Wired* (5 August 2018) <https://www.wired.co.uk/article/tupac-michael-jackson-billie-holiday-dead-celebrity-holograms> accessed 20 February 2022.

[23] Matthew Dunne-Miles, 'Deepfakes, Dead Relatives and Digital Resurrection', *The Face* (6 April 2021) <https://theface.com/society/deepfakes-dead-relatives-deep-nostalgia-ai-digital-resurrection-kim-kardashian-rob-kardashian-grief-privacy> accessed 20 February 2022.

[24] Jimi Famurewa, 'Inside the Bitter war to Bring Tupac and Michael Jackson Back to Life', *Wired* (5 August 2018) <https://www.wired.co.uk/article/tupac-michael-jackson-billie-holiday-dead-celebrity-holograms> accessed 20 February 2022.

[25] Adrienne Matei, 'What Should Happen to Our Data When We Die?' (New York Times, 24 July

erary executor, over whether permission for the synthesised voice had been granted.[26] This was followed by a huge backlash on social media, questioning whether such an insertion was ethical, appropriate, or distasteful.[27] The most recent instance where the deceased's reincarnation was used is a fake episode of the podcast Joe Rogan Experience. Rogan spoke to the late Steve Jobs, whose AI-generated voice interacted with Rogan for 19 min and appeared quite natural.[28]

Ghostbots have potential beyond entertainment in terms of historic preservation, education, and digital archiving, from the reincarnation of the surrealist artist Salvador Dalí, who snaps selfies with museum visitors,[29] to the creation of interactive biographies with Holocaust survivors as a means of preserving their testimony for future generations through predictive algorithms.[30]

There is increasing commercialisation of deepfake technology for the deceased. A trajectory is visible from simple memorial sites for the deceased, often paid for on monthly plans,[31] to today's and tomorrow's ghostbots. Companies such as Eternime are experimenting with AI technology to create posthumous avatars through the collection of 'geolocation, motion, activity, health app data, sleep data, photos, messages that users put in the app' from the deceased's smartphone.[32] In 2020, Microsoft was granted a patent for creating chatbots that may correspond to a present entity, such as oneself, a friend, a relative, or even a historical or fictional character. It would be based on 'images, voice data, social media posts and electronic messages' with the option of rendering in 2D or 3D.[33] Tim O'Brien, Microsoft's General Manager of AI at the time, acknowledged that this was a disturbing piece of technology, stated that there were currently no plans to develop the chatbot technology since the original patent application predated Microsoft's current AI ethics review procedures.[34]

These ghostbots vary greatly in sophistication. The deepfake technology of My Heritage's DeepNostalgia is relatively unsophisticated, only allowing for simplistic movements – such as blinking, nodding or smiling – of single headshots. Possibly attempting to stave off potential privacy challenges, abuse or controversy, MyHeritage deliberately did not add a speech element to their created videos.[35] In a blog post published to coincide with the service launch, MyHeritage asked users to only 'use this feature on your own historical photos, and not on photos featuring living people without their permission'.[36] This does not seem to have prevented people from using DeepNostalgia to create bots from statues and illustrations.[37]

A more recent service, HereAfter AI, allows users to record their life stories and answer some commonly posed questions and themes, which then serve as a basis for post-mortem interaction.[38] Users can also upload photos to illustrate the story. After their death, designated family members can access those memories by posing life story questions to the app. The app replies in the author's voice with stories, memories, and advice and shows uploaded photos. Once again, the technology is fairly unsophisticated – apparently based on rule-based logic as opposed to complex machine learning - and does not create a 'full-blown' ghostbot.

The above-referenced podcast featuring Steve Jobs shows a higher level of sophistication with speech and interactive elements. Currently, the more bespoke the deepfake (cf the living deepfake of Tom Cruise noted above), the more sophisticated the tech available, and the result tend to be. However, the rise and vast popularity of AI large generative models used to generate images and videos in 2022, although not obviously yet being employed to create replicas of the dead, is likely to mean that sooner rather than later, ghostbot technology will become ubiquitous, democratised, professional and monetised.

The much hyped 'metaverse' may become an obvious locus for the exploitation of ghostbot technologies. A metaverse world, Somnium Space, has already developed a 'Live Forever' option which allows a virtual version of a person (avatar) to become 'eternal' and communicate with loved ones on death.

2021), https://www.nytimes.com/2021/07/24/style/what-should-happen-to-our-data-when-we-die.html accessed 20 February 2022.

[26] Ibid.

[27] Marisa McVey, 'Deepfakes and the Dead: The Case of Anthony Bourdain', (10 August 2021, Modern Technologies, Privacy Laws and the Dead), https://thefutureofprivacylaw.wordpress.com/2021/08/10/deepfakes-and-the-dead-the-case-of-anthony-bourdain/ accessed 20 February 2022.

[28] ODSC Team, 'AI Used to Create a Fake Podcast with Joe Rogan and Steve Jobs', (17 October 2022, *Open Data Science*), https://opendatascience.com/ai-used-to-create-a-fake-podcast-with-joe-rogan-and-steve-jobs/ accessed 20 February 2022.

[29] Dami Lee, 'Deepfake Salvador Dalí Takes Selfies with Museum Visitors', *The Verge* (10 May 2019) <https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum> accessed 20 February 2022.

[30] 60 Minutes 'Letting Future Generations Speak with Holocaust Survivors', *CBS News* (21 January 2021) <https://www.cbsnews.com/video/from-the-60-minutes-archive-letting-future-generations-speak-with-holocaust-survivors/#x> accessed 20 February 2022.

[31] E.g. Forever Misses, https://www.forevermissed.com/ or GatheringUs, https://www.gatheringus.com/. Never Gone, http://never-gone.com/ accessed 20 February 2022.

[32] Isobel Asher Hamilton, '2 Tech Founders Lost their Friends in Tragic Accidents. Now They've Built AI Chatbots to Give People Life after Death', *Business Insider* (17 November 2018) < https://www.businessinsider.com/eternime-and-replika-giving-life-to-the-dead-with-new-technology-2018-11?r=US&IR=T> accessed 20 February 2022.

[33] See details at n 35 below.

[34] Edina Harbinja, Lilian Edwards and Marisa McVey 'Chatbots Resurrect the Dead: Legal Experts Weigh in on 'Disturbing' Technology', *The Conversation* (1 March 2021) <https://theconversation.com/chatbots-that-resurrect-the-dead-legal-experts-weigh-in-on-disturbing-technology-155436> accessed 20 February 2022.

[35] Alex Hern, 'Deep Nostalgia: 'Creepy New Service uses AI to Animate Old Family Photos', *The Guardian* (1 March 2021) <https://www.theguardian.com/technology/2021/mar/01/deep-nostalgia-creepy-new-service-ai-animate-old-family-photos> accessed 20 February 2022.

[36] MyHeritage Blog <https://blog.myheritage.com/2021/02/new-animate-the-faces-in-your-family-photos/> accessed 20 February 2022.

[37] Alex Hern, 'Deep Nostalgia: 'Creepy New Service uses AI to Animate Old Family Photos', *The Guardian* (1 March 2021) <https://www.theguardian.com/technology/2021/mar/01/deep-nostalgia-creepy-new-service-ai-animate-old-family-photos> accessed 20 February 2022.

[38] HereAfter AI, https://www.hereafter.ai/.

The ambition in the founder's words was, 'Literally if I die—and I have this data collected—people can come or my kids, they can come in, and they can have a conversation with my avatar, with my movements, with my voice. You will meet the person. And you would maybe for the first 10 min while talking to that person, you would not know that it's actually AI. That's the goal.'[39] Sychov, the founder, also notes that the amount of data they potentially could collect in the metaverse is 100 to 300 times more than the data collected through a phone. This includes data about how user's fingers, mouth, eyes, and entire body move.

3. Harms caused by ghostbots and legal responses

Ghostbots are a new technology, and with every example of such, arguably, opportunities arise for misuse as well as advantage. The law tends only to become involved if serious economic and sometimes emotional or dignitary harms result. Ghostbots, in their nature, cannot cause physical damage, but several other types of potential harm can be discerned.

First, emotional distress may result if relatives of the deceased become psychologically dependent on a ghostbot and unable to move on from their grief. On this, the jury is still out, and the law may not regard it as its province. Ghostbots may become damaging conduits for racist or abusive messages 'from the grave' if they learn such from either their training dataset or the environment in which they are trained - compare the chatbot Taybot built by Microsoft, which was placed in the abusive environment of Twitter, soon learned to parrot racist and misogynist discourse.[40] Racist taunts from a beloved grandparent might well be regarded as more damaging than insults from a passing stranger on Twitter. However, the law could almost certainly subsume such harms under existing laws, such as public order, equality, race and religious hate laws, defamation (of someone other than the deceased themselves) and verbal assault. Laws such as the Online Safety Bill being developed in the UK,[41] which attempts to place care duties on platforms and intermediaries, might relatively easily be adapted to the ghostbot world.

Pornography laws, including non-consensual use of intimate images ('revenge porn'[42]) might also come into play. For example, one can imagine a scenario where a celebrity is 'reincarnated' as a ghostbot to provide sexualised entertainment. It is already common for such sexual deepfakes to be created without permission, either from existing pictures or using machine learning deepfake techniques.[43] Indeed, around 90% or more of deepfakes fall into this category.[44] UK pornography laws should apply *mutatis mutandum* where applicable; there is an interesting question if a sexual ghostbot might be deemed extreme pornography as involving necrophilia,[45] meaning that its mere possession would be a serious crime. Other offenders might also include a platform where the ghostbot was stored or accessed and the person who creates ('makes') the ghostbot (which might gratifyingly exert a chilling effect over the entire endeavour).

Economic harms may be more likely to provoke legislative concern. Ghostbots, especially where the service is on the face of it free to the user, might well be used to market goods or services to surviving relatives or heirs. The vulnerability invoked by grief and memory might make undue influence or deception relatively likely. Subliminal messaging or product placement might also feature in the business models. Such phenomena are already widely seen in the context of marketing by toys and cartoon characters to children as vulnerable and unsafeguarded consumers. For example, it is well documented that junk food is marketed to children in their media, especially during cartoons, with adverse effects on their nutritional health.[46] Digital online influencers have also presented regulators with significant transparency issues and undisclosed marketing ties.[47] The regulation of such deceptive online marketing remains highly controversial and diverse globally. These business models are already emerging in ghostbot world. In personal interaction with the app Replika, which is marketed as useable to create interactive post-mortem chatbots, attempts were made within minutes of one author setting up a 'replica', to sell (a) subscription pornography in which NSFW pictures of the avatar would be shared and (b) a Samsung phone (in response to an unprompted question from the bot as to what my phone was). Again, existing laws

[39] Maxwell Strachan 'Metaverse Company to Offer Immortality Through 'Live Forever' Mode' (*Vice*, 13 April 2022), https://www.vice.com/en/contributor/maxwell-strachan accessed 20 February 2022.

[40] See James Vincent, 'Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day', (*The Verge*, 24 March 2016), https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist accessed 20 December 2022.

[41] See for England and Wales, the Communications Act 2003, the Malicious Communications Act 1988 and Protection from Harassment Act 1997. These laws are likely to be amended under the forthcoming Online Safety Bill.

[42] Section 33 of the Criminal Justice and Courts Act 2015, c 2 cannot apply here as the dead cannot give or withhold consent in English law. The protection of the deceased against revenge porn is, however, now available in New York.

[43] DeepNude App https://app.deepnude.cc/upload; Samantha Cole, 'This Horrifying App Undresses a Photo of Any Woman With a Single Click' (*Vice*, 26 June 2019), https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman accessed 20 February 2022.

[44] Sensity, 'The State of Deepfakes 2020: Updates on Statistics and Trends', March 2021, https://sensity.ai/reports/ accessed 20 February 2022.

[45] For England and Wales, see Criminal Justice and Immigration Act 2008, Section 7 (c): 'An image falls within this subsection if it portrays, in an explicit and realistic way. an act which involves sexual interference with a human corpse'. It seems unlikely an English court would take this interpretation.

[46] See e.g. Stuart Elliott 'Product Placement Moves to Cartoons', *NY Times*, 21 October 2004 at https://www.nytimes.com/2004/10/21/business/media/product-placement-moves-to-cartoons.html, accessed 22 December 2022.

[47] See the continuing action the UK Competition and Markets Authority has taken since 2018 to try to enforce disclosure and advertising rules against online influencers: see https://www.gov.uk/government/news/celebrities-and-social-media-stars-investigated-for-not-labelling-posts. See further Catalina Goanta and Sophia Ranchordas, eds, *The Regulation of Social Media Influencers* (Edward Elgar, 2020).

may arguably cover potential harms here: relating to offensive communications, fraud, consumer protection, and advertising. Tort and product liability might also be relevant regimes where the manufacture, delivery or use of a ghostbot leads to harm. As we will see below, the current EU AI Act proposal introduces a duty of transparency concerning deepfakes and chatbots. Such 'labelling' proposals have been tried before in the digital world, notably in relation to spam,[48] but with little discernible impact.

In addition to the harms of emotional dependence, abusive communications and deception for commercial purposes, it is worth considering if there is potential harm to the deceased's antemortem persona. This is one of the most controversial questions in post-mortem rights scholarship due to the issues raised of the subject of the harm, the nature of the harm and backwards harm causation. Some philosophers suggest that harming the deceased may be possible. Stokes considers digital remains' impact on the ontological and ethical status of the dead. He argues that these artefacts allow persons to persist as 'ethical patients' after biological death and that this persistence function of digital remains creates an obligation not to delete them. He then submits convincingly that these artefacts enjoy 'a claim to moral regard akin to that of corpses'.[49] Regarding the nature of the harm and causation, Pitcher argues that an antemortem person can be harmed by a post-mortem event as much as by an event that occurs antemortem since 'the occurrence of the event makes it true that during the time before the person's death, [he] was harmed - harmed in that the unfortunate event was going to happen.'[50] Feinberg refines Pitcher's position by defining his thwarted posthumous interests as 'doomed interests'.[51] Feinberg then goes on to submit that the antemortem person is harmed 'at the point, well before [his] death, when the person had invested so much in some postdated outcome that it became one of [his doomed] interests.'[52] Building on this school of thought, legal scholar Davey argues that harm to the antemortem person, inter alia, occurs in the form of the 'chilling effect' in life due to the risk of post-mortem privacy invasion, as well as the prospect of a secret being revealed upon death.[53] Harbinja shares these views and has developed her conception of post-mortem and postmortal privacy based on harm caused to the antemortem persona, her autonomy, dignity, and identity interests, and her 'forced' immortality-by-proxy.[54]

3.1. *Ownership and control of the personal data of ghostbots*

The more interesting legal questions about ghostbots move beyond the familiar harms and equally familiar laws canvassed above into complex notions of post-mortem ownership and control. We examine these below, drawing primarily on EU data protection law and considering art 8 of the European Convention on Human Rights (ECHR) and certain national laws.

Ghostbots are, as noted above, a recreation in some interactive form of a deceased person's appearance, voice or personality after their death. Extensive amounts of data are needed to produce ghostbots. These may include emails, photos, videos, personal messages, social media posts, tweets, voice calls and voicemails left by the deceased. In data protection terminology, these all contain personal data, some of them sensitive personal data (relating to, for example, race, religion or sexuality, under art 9 of the GDPR). Data subjects have the right to control their personal data during life (a 'control' paradigm). Should they (somehow) be granted similar rights after death, hence being able to control the recreation of their personality after death? If so, it logically follows that data subjects should have the right to veto their appearance as ghostbots after death, although a mechanism to exercise this control post-mortem would need to be found, especially if it was the heirs who wanted to build the bot: perhaps by inserting an enforceable request not to become bots ('do not bot me') in their wills? The problem of who would enforce such a request, given that the heir might well also be the estate administrator, remains.

Alternately, at present, whether by will or intestate succession, heirs inherit the worldly goods, tangible (e.g. their car) and intangible (e.g. their copyrights in their letters) of the deceased. Should heirs also inherit control over their personal data (a 'property' paradigm)? If so, it would follow that *heirs* should have the exclusive right to create ghostbots, or at least to license their creation, even though the letters, voicemails, Facebook posts, etc., might be found in the hands of multiple third parties or platforms. Arguably heirs would also be entitled to stop anyone else (friends, more distant relatives - or perhaps in the case of deceased celebrities, producers, entrepreneurs or fans) from creating competing versions.

These apparently esoteric questions are very likely to become mainstream fairly soon, given the rapid development and monetisation of ghostbot services, celebrity replicas and virtual realities. Just as 2022 has already seen a considerable amount of money devoted to, and made out of, the creation of digital holograms of the living members of the band Abba as they appeared in their 30 s ('ABBAtars')[55], future years are

[48] See EU Electronic Commerce Directive 2000/31/EC arts 6 and 7.

[49] Patrick Stokes, 'Deletion as Second Death: The Moral Status of Digital Remains' *Ethics and Information Technology* 17:4 (December 2015), 237-248; or for a more abstract account of the survival of the deceased's personhood, see Patrick Stokes, 'Are there dead persons?' *Canadian Journal of Philosophy*, 49(6), 755-775. doi:10.1080/00455091.2018.1442402.

[50] George Pitcher, 'The Misfortunes of the Dead', 21 AM. PHIL. Q. 183 (1984), 188.

[51] Joel Feinberg, *The Moral Limits of the Criminal Law Volume 1: Harm to Others* (1987, Oxford University Press USA). 91 - 92.

[52] Ibid, 92.

[53] Davey 180 - 181

[54] Edina Harbinja 'The "New(ish)" Property, Informational Bodies and Postmortality', in M Savin-Baden and V Mason-Robbie, (eds.), Digital Afterlife: Death Matters in a Digital Age (Taylor & Francis, 2020); *Digital death, digital assets and post-mortem privacy: theory, technology, and the law* (EUP, 2022), Chapter 6.

[55] See https://abbavoyage.com/. See Theo Tzanidis and Stephen Langston, 'Are digital avatars the future of music touring?' (*Independent*, 22 April 2022) https://www.independent.co.uk/arts-entertainment/music/features/metaverse-digital-avatars-music-concert-abba-tours-b2062307.html accessed 20 February 2022. They suggest that as landmark bands age, digital replicas as touring substitutes may become the norm: there seems no reason

likely to see a great deal of money put into the recreation of not just Abba, but more ordinary folk, after their death.

Whose side does the law take right now, the deceased or the heir? At present, it seems largely axiomatic that no one owns personal data, certainly not the deceased.[56] Who 'owns' data at all is a difficult issue to start with.[57] Some particular types of data that fall under the head of creative works, e.g. texts, emails, images - might be regarded as intellectual property in the form of copyright, although this will not always be the case (e.g. requirements of novelty may prevent brief texts such as 'Hello!' being copyrightable).[58] However, we will not focus on copyright in this paper, and we invite the reader to consider some of our earlier work in this area.[59] A few esoteric types of information, such as trade secrets or 'hot news', can be subject to quasi-property treatment in US common law.[60] However, this type of information is largely irrelevant to the creation of ghostbots. There have been attempts lately to squeeze what might be called data-based goods into novel property regimes. A recent example is an idea to create a 'third category of property' in English law to accommodate desires for clearer ownership rights in cryptocurrency assets.[61] This rather opportunistic proposal could pave the way for the proposals for propertisation of other intangibles outside of conventional intellectual property categories, including personal data, although overwhelmingly, European privacy scholars are resistant to this idea.[62]

In general, there is a well-established lack of legal protection for the deceased's personality, privacy, data or dignity after death.[63] There are, however, an increasing number of exceptions to this principle. Recital 27 of the GDPR, for instance, does leave it open to individual member states to provide post-mortem privacy protection if they wish. Erdos has usefully analysed the large and increasing number of post-mortem data protection laws in his recent work.[64] These post-mortem data protection laws have interesting implications, not for the privacy rights of the deceased directly but for the rights of relatives or heirs over post-mortem ghostbots.

Imagine a ghostbot is built, based perhaps on public Facebook posts and comments from multiple hands, scraped by a friend rather than an heir of the deceased. The bot tells stories in style akin to HereAfterAI, which seems to impugn the memory of the deceased or perhaps of relatives or friends of the deceased whom the builder of the bot did not like. It might tell stories about how the surviving spouse was unfaithful or unhelpful or how the child was feckless with money or deceived tax authorities. Whether true or false, based on the current law in Italy, heirs might conceivably be able to invoke the right to be forgotten under the GDPR article 17, and possibly seek deletion of the entire bot as made of personal data 'relating to' the deceased – or perhaps just ask for certain data to be removed from its programming.[65] Would it make any difference if it was argued that the data related not just to the deceased but to other living persons?[66] Or that there was a public interest in revealing details of proven criminality?[67] Fascinating issues might also arise if 'new facts' were derived by machine learning from a corpus of post-mortem texts or im-

why this hypothesis should not extend to after band members die. Indeed, as the article notes, AI models could also compose new music in the style of the deceased songwriters or musicians. (Ownership of such music is left as an exercise to the reader.)

[56] Edina Harbinja, 'Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?'10 (2013) SCRIPTed 19.

[57] See our earlier work on this topic: Harbinja, *Digital death, digital assets and post-mortem privacy: theory, technology, and the law* (n 54), chapter 6; Lilian Edwards and Edina Harbinja 'Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World', (2013) 32(1) Cardozo Arts & Ent. L.J. 111; '"Be Right Back": What Rights Do We Have Over Post-Mortem Avatars of Ourselves?' in L Edwards, E Harbinja and B Schafer (eds.), Future Law, Emerging Technology, Regulation and Ethics (Edinburgh: Edinburgh University Press, 2020); Harbinja (n 54).

[58] In the UK, for instance, single words have been refused copyright protection, see word 'Exxon' in *Exxon Corp. v. Exxon Insurance Consultants International Ltd* [1982] Ch. 119.

[59] Harbinja (n 57), Edwards and Harbinja (n 21).

[60] Harbinja (n 57), chapter 2.

[61] Law Commission, 'Digital assets Consultation paper', Law Com No 256, 28 July 2022.

[62] Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of Our Identity', in Lucie M.C.R. Guibault & P. Bernt Hugenholtz, eds. *The Future of Public Domain: Identifying the Commons in Information Law* (Kluwer Law International, 2006) 223; Nadezhda Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?', 10 J.L. & ECON. REGULATION 64 (2017); Thomas Hoeren & Philip Bitter, 'Data Ownership is Dead: Long Live Data Ownership', 40 EUR. INTELL. PROP. REV. 347 (2018); Henry Pearce, 'Could the Doctrine of Moral Rights be Used as a Basis for Understanding the Notion of Control within Data Protection Law?', 27 INFO. & COMM. TECH. L. 133, 156-65 (2018); Steven H. Hazel, 'Personal Data as Property', 70 SYRACUSE L. REV. 1055 (2020); Harbinja (n 57).

[63] See e.g. J C Buitelaar, 'Post-Mortem Privacy and Informational Self-Determination' (2017) 19(2) Ethics and Information Technology, 129; Tina Davey, *Until Death Do Us Part: Post-mortem Privacy Rights for the Ante-mortem Person* (PhD thesis, University of East Anglia, 2020); Edwards and Harbinja (n 21), Edina Harbinja, 'Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?'10 (2013) SCRIPTed 19; 'Post-Mortem Privacy: Theory, Law, and Technology' (2017) 31(1) International Review of Law, Computers and Technology, 26; 'The "New(ish)" Property, Informational Bodies and Postmortality', in M Savin-Baden and V Mason-Robbie, (eds.), Digital Afterlife: Death Matters in a Digital Age (Taylor & Francis, 2020); Harbinja, *Digital death, digital assets and post-mortem privacy: theory, technology, and the law* (n 54); Gianclaudio Malgieri, 'R.I.P: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects Between Theoretical Scenarios and National Solutions' in R Leenes, R van Brakel, S Gutwirth and P de Hert (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing, 2018); Tal Morse and Michael Birnhack, 'The Posthumous Privacy Paradox: Privacy Preferences and Behavior Regarding Digital Remains' (2021) *New Media and Society*, 1.

[64] See David Erdos Dead ringers? Legal persons and the deceased in European data protection law' 40 (2021) Computer Law & Security Review; and Harbinja, *Digital death, digital assets and post-mortem privacy: theory, technology, and the law* (n 54).

[65] Italy, Personal Data Protection Code Legislative Decree 196/2003 as amended by Legislative Decree101/2018, art. 2(3).

[66] *Dzhugashvili v. Russia* (2014) ECHR 1448, *Éditions Plon v France* (2004) ECHR 200, *Putistin v. Ukraine* (2013) ECHR 1154; *ML v Slovakia* (2021) ECHR 821

[67] *Google Spain* (Case C-131/12); *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-136/17).

ages: e.g., someone repeatedly visited a certain place seen in the background of photos or often mentioned an ex-partner in WhatsApp messages. Would this 'new personal data' also be subject to any rights of the heirs to seek erasure?[68] This becomes even more fascinating if we consider the data used to create a ghostbot in a metaverse world. Could heirs request its portability under GDPR art 20 to another metaverse world?

Contrast this to the UK, where privacy and data protection laws do not extend protection to heirs after death. Data protection rights would fall away, and similarly, any right of action under defamation[69] or misuse of private information (formerly breach of confidence)[70] would not be available to the deceased's personal representatives.[71] Basically, relatives or friends would have no remedies under privacy, data protection or defamation law, even if the claims of the ghostbot were lies and damaging to reputation.

3.2. *Article 8 of the European convention of human rights*

Considering the European level further, we might ask if any help can be drawn from the right to protection of one's right to private life under article 8 of the European Convention of Human Rights (ECHR), which has been interpreted in case law to give rights over inter alia image, reputation, identity and records.[72] As with the GDPR (which is to some extent derived therefrom), article 8 of the Convention does not extend post-mortem, and rights cannot be transferred to representatives.[73] However, a living person's rights under article 8 may, in certain circumstances, be infringed by damage to the reputation of a deceased member of that person's family.[74] For example, in *ML v Slovakia*, a parent successfully argued their rights to privacy had been breached by the publication several years after his death of 'tawdry' photos of their son, a priest who had committed suicide after a criminal conviction.[75] Based on these cases, arguably, a family member might be able to invoke privacy rights, including a 'right to be forgotten', in relation to disclosures made by a ghostbot.[76]

Further complexity is added if we consider that competing ghostbots might be made from the public data of the deceased by, respectively, a family member and a friend. Might a relative have a right to claim under article 8 that their version of the ghostbot should be kept up while the competing friend's version is taken down? Would anyone have the right to decide which was the more faithful depiction of the deceased's persona, and would this even be relevant in the context of article 8 given the human right pertains to the live claimant and not the deceased? These exciting questions intuitively seem poorly solved by referring to the law of data protection, privacy or human rights[77].

3.3. *National laws*

Protection of dignity and personality is guaranteed by the constitutions of certain countries, such as Germany.[78] The right to image is also protected more broadly in France, for instance, than in the UK. In the US, publicity rights may be violated, especially for celebrities and all other individuals in some states where this protection exists and in some US states, this protection extends to a degree of post-mortem term.[79] The hybrid 'post-mortem privacy' approach is increasingly acknowledged in the US model and state law,[80] French law,[81] recent and upcoming laws elsewhere in the world,[82] and numerous

[68] Similar issues would arise in Estonia, where heirs would be able to withdraw consent for the processing of personal data and seek prohibition of further processing and sharing of the ghostbot. Estonia, Personal Data Protection Act 2019, s. 9.

[69] Under the Defamation Act 2013 c. 26 and the relevant case law.

[70] See *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457 (6 May 2004). Misuse of private information was first recognised as a distinct civil tort in *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB)[4], by Tugendhat J, as distinct from breach of confidence.

[71] *Baker v. Bolton*, (1808) 170 Eng. Rep. 1033 (K.B.). The principle has later been revised and only pertains to causes of action for defamation and certain claims for bereavement. See generally Law Reform (Miscellaneous Provisions) Act 1934, c. 41, The Race Relations Act 1976, c. 74, Sex Discrimination Act 1975, c. 65, Disability Discrimination Act 1995, c. 50, and Administration of Justice Act 1982, c. 53.

[72] *von Hannover v. Germany (no. 2)*, Grand Chamber judgment of 7 February 2012, § 96; see ECtHR guidance on art 8 case law at https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

[73] Davey has offered a detailed outlook of this in chapter 6 of her thesis, Davey (n 63).

[74] *Jakovljević v. Serbia* (2020), Application no. 5158/12.

[75] *Dzhugashvili v. Russia* (2014) ECHR 1448, *Éditions Plon v France* (2004) ECHR 200, *Putistin v. Ukraine* (2013) ECHR 1154; *ML v Slovakia* (2021) ECHR 821; for more, see Davey ibid, 184.

[76] Compare *ML v Slovakia*, supra.

[77] They are similarly badly solved by reference to laws about the treatment of dead bodies, the protection of graves against desecration, medical confidentiality post-mortem, publicity rights, image and moral rights etc. See Edwards and Harbinja (n 57) and Davey (n 63).

[78] 'Human dignity shall be inviolable.' Article 1, Basic Law for the Federal Republic of Germany (as amended July 2002) [Germany], 23 May 1949, available at: https://www.refworld.org/docid/3ae6b5a90.html accessed 20 February 2022.

[79] For an overview and comparison, see Edwards and Harbinja (n 57); David G. Post, 'Territoriality, Jurisdiction, and the Right(s) of Publicity' (March 30, 2019). *Columbia Journal of Law & the Arts*, Vol. 42, No. 3, 2019, Available at SSRN: https://ssrn.com/abstract=3380652; Douglas G. Baird, 'Does Bogart Still Get Scale? Rights of Publicity in the Digital Age' (April 2001). U Chicago Law & Economics, Olin Working Paper No. 120, Available at SSRN: https://ssrn.com/abstract=268516.

[80] US Uniform Law Commission, 'Fiduciary Access to Digital Assets Act, Revised (2015): www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%.

[81] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique; for a comparison between the French and US approach, see Lucien Castex, Edina Harbinja and Julien Rossi, 'Défendre les vivants ou les morts? Controverses sous-jacentes au droit des données post-mortem à travers une perspective comparée franco-américaine' 4(210) (2018) Réseaux 117.

[82] Uniform Law Conference of Canada, Uniform Access to Digital Assets by Fiduciaries Act (2016) www.ulcc.ca/images/stories/2016_pdf_en/2016ulcc0006.pdf; The most recent addition is the Personal Information Protection Law of the People's Republic of China ('PIPL') 2021, article 49 provides close relatives of the deceased to exercise the right to access, correct, and delete the personal information of the deceased, unless otherwise arranged before the death of the deceased.

data protection statutes, as noted above.[83] The discussion is ongoing, and a degree of law reform may even be forthcoming in England and Wales, one of the jurisdictions least prone to ascribing rights to the dead.[84] It is also important to note that platforms such as Facebook, Google and Apple now allow users to make at least a minimum disposal of what happens to their platform-hosted data after they are dead by 'digital wills' such as Legacy Contact or Inactive Account Manager - although it remains unclear what will happen if these devices come into conflict with 'real' wills or default rules on intestacy.[85]

We have argued on multiple occasions that the regulation of post-mortem privacy and data protection needs to be re-examined. The circumstances of the online world – notably, the growth in volume and importance of personal data, the amount of time spent online and its importance to identity, and the prevalent loss of control of that data during life to platforms and intermediaries - have undermined the standing legal norm that rights to control over privacy and personality should end on death. We do not propose to rehearse these arguments again in detail here.[86] As public sentiment has moved towards greater consideration of post-mortem rights, though, rules have become ragged around the edges and EU law poorly harmonised, as Erdos' work shows. In their latest article, where they consider the taxonomy of digital remains, Birnhack and Morse submit that the law should protect the 'reasonable expectations of the living regarding their post-mortem condition, subject to balancing them with competing interests and rights of the living.'[87] This could become a standard for review of the GDPR and article 8 ECHR approaches.

Alternatively, should we look to a bespoke law to regulate ghostbots in various ways (privacy, property, consumer protection, vulnerability)? It seems unlikely that we are quite yet at the point where legislatures will regard this as a priority. However, we turn in the next section to look at two partial legislative solutions to some of the problems around ghostbots, so far canvassed: one from the EU and one from New York.

4. Emerging ghostbot laws

4.1. *The New York law*

In the search for appropriate regulation of ghostbots, we might expand our horizons across the Atlantic. New York's recent law on the right to publicity is an exciting example of a law that directly relates to deepfakes and deceased persons (although restricted to the category of celebrities). It was signed into law by Governor Andrew Cuomo in late 2020 and took effect in May 2021.[88] Until this legislation, New York's right of publicity statute only protected living persons.[89]

The state's right of publicity provides protection for two categories of deceased celebrities. First, it extends to any 'deceased personality', i.e., any deceased natural person domiciled in the state of New York at the time of death and whose' name, voice, signature, photograph or likeness' has a commercial value at the time of death, regardless of whether that person used their likeness for commercial purposes during life.[90] The right is extended for forty years after death.[91] However, it requires a successor to register a public claim with the NY Secretary of State in order to be enforceable[92] – similar to that of the 'registration prior to enforcement' requirement in US federal copyright law[93] or the 'successor-in-interest' registry in Californian law.[94] This right of publicity may be exercised by a decedent's estate as well as anyone who inherits or owns at least 51% of the rights.[95]

Secondly - and most uniquely - there is a further prohibition on the use of digital replicas of 'deceased performers' – i.e., a deceased natural person domiciled in the state of New York at the time of death who, 'for gain or livelihood, was regularly engaged in acting, singing, dancing, or playing a musical instrument'.[96] While post-mortem publicity rights are protected in some other states (most notably California), no other state extends this protection to digital replicas. Under the New York law, digital replicas are defined as

> *Newly created, original, computer-generated, electronic performance by an individual in a separate and newly created, original expressive sound recording or audiovisual work in which the individual did not actually perform, that is so realistic that a reason-*

[83] Erdos (n 64).

[84] See recently; Law Commission, 'Making a will' (Consultation paper 231, 2017) www.s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/07/Making-a-will-consultation.pdf; also the suggestion of the Online Safety Bill (OSB) Joint Committee that access of administrators to the data of the deceased on platforms should be facilitated as part of the Online Safety Bill, Paragraphs 463 - 464, Joint Committee on the Draft Online Safety Bill, 'Draft Online Safety Bill: Report of Session 2021–22', HL Paper 129, HC 609, Published on 14 December 2021); contrast the Digital Devices (Access for Next of Kin) Bill, a Private Members Bill which had its first reading in the House of Commons in January 2022 and which seeks to grant the next of kin the right to access digital devices of a person on their death or incapacity. Our view is that the latter is a highly flawed Bill which fails to take any account of a balance to be struck between the privacy of the deceased and the interests of the heirs and administrators.

[85] See Edwards and Harbinja (n 20), Harbinja (n 44).

[86] Edwards and Harbinja (n 20), Harbinja (n 44).

[87] Michael D. Birnhack and Tal Morse, 'Digital Remains: Property or Privacy?' *International Journal of Law and Information Technology* (Forthcoming, 2023), Available at SSRN: https://ssrn.com/abstract=4254683 or http://dx.doi.org/10.2139/ssrn.4254683.

[88] Legislation ref: S5959D/A5605C.

[89] The new law also provides for a comprehensive inter vivos right of action for the unlawful dissemination or publication of a 'sexually explicit depiction of an individual' (N.Y. Civ. Rights § 52-c (as amended by S5959D)), which has been interpreted as prohibiting so-called non-consensual deepfake pornography.

[90] N.Y. Civ. Rights § 50-f(1)(b) (as amended by S5959D).

[91] N.Y. Civ. Rights § 50-f(2)(8) (as amended by S5959D).

[92] N.Y. Civ. Rights § 50-f(1)(c) (as amended by S5959D).

[93] Matthew F. Ferraro and Louis W. Tompros, 'New York's Right to Publicity and Deepfakes Law Breaks New Ground' (April 2021) *The Computer and Internet Lawyer* 38(4).

[94] California Civ. Code § 3344.1

[95] Dentons, 'New York's new post-mortem publicity rights law: What does it mean for your estate? What does it mean for your advertising campaign?' (2020) <https://www.dentons.com/en/insights/articles/2020/december/8/new-yorks-new-post-mortem-publicity-rights-law-what-does-it-mean-for-your-estate#footnote4>.

[96] N.Y. Civ. Rights § 50-f(1)(a) (as amended by S5959D).

able observer would believe it is a performance by the individual being portrayed and no other individual.[97]

There are, of course, exceptions to the prohibition of these digital replicas. For instance, the digital remastering of sound recordings does not constitute a replica.[98] Crucially, in order to avail of the statute's protection, the digital replica must also be used in a deceptive manner. So, producing a 'conspicuous disclaimer' that the replica was not authorised by the rightsholder is sufficient to avoid liability.[99] Nevertheless, advertisers on social media platforms need to tread carefully when using the likeness of any deceased celebrity in posts without permission, in case such use could be viewed as an endorsement of the advertiser's products and services.[100]

The justification for this new legislation seems to be in recognition of the need for the right of publicity as a control function, acknowledging that though it remains within the bounds of property rights, the right of publicity is not simply a tangible property asset.[101] If a celebrity or their successor does not want to commercialise the right of publicity, they should not be compelled to do so. Notably, the law also acknowledges the necessary balance between the individual right of publicity and free speech considerations under the First Amendment of the US Constitution, which exempts public interest or satirical content applications or usage in literary or artistic works.[102] The Act is limited by only giving rights to famous persons or performers and their successors and not to the (deceased) general public. Nevertheless, the law has been described as 'pathbreaking', and commended by the Screen Actors Guild for protecting performers from exploitation.[103] Overall, while more than 20 other US states also recognise the post-mortem right to publicity - with each law varying on duration and domicile criteria[104] - New York paves the way in terms of extending these protections to celebrity ghostbots.

4.2. *The EU AI Act*

The European Commission released a proposed Regulation on Artificial Intelligence[105] (the 'AI Act') on 21 April 2021. The Act sets out harmonised rules for the development, placement on the market, and use of AI in the European Union (EU). The Act is wide-ranging, but the most proximate point here is the novel requirement for transparency for deepfakes and chatbots.[106]

Article 52 defines deepfakes as an 'AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake')', and requires that anyone putting such a system into use (in AI Act terminology a 'user' – but actually more commonly thought of as a deployer) discloses[107] that the content has been artificially generated or manipulated.[108] This definition certainly seems to cover ghostbots. Deployers of ghostbots in the EU who failed to provide such warnings would, in theory, be subject to potentially large fines as well as the possibility of the system being withdrawn from the EU market. However, the history of policing online labelling in the EU, e.g. in the context of spam email under the E-Commerce Directive[109] is poor, and it seems dubious that much effort would be made to police this rule where ghostbots were made or hosted and accessed on servers, outside the EU.

The key question when looking at this as a model for regulation (note the EU AI Act will no longer automatically become law in the UK post-Brexit) is whether a transparency obligation is appropriate, sufficient, or indeed necessary to safeguard consumers and other end-users against harm caused potentially by ghostbots of the kind we canvassed above, such as emotional dependence, deception for commercial purposes, or abusive communication. Deepfakes and chatbots are pointedly not defined in the Act as 'high-risk' AI, where the bulk of the Act's obligations fall. For 'high-risk' AI, providers must certify that the system has been built according to certain technical standards designed to produce fair, safe and non-discriminatory systems. This technical mandate approach has its criticisms,[110] but it would be an advance on simple warnings which require no actual care about the creation of the product. On the other hand, it can easily be ar-

[97] N.Y. Civ. Rights § 50-f(1)(c) (as amended by S5959D).
[98] N.Y. Civ. Rights § 50-f(1)(c) (as amended by S5959D).
[99] N.Y. Civ. Rights § 50-f(2)(b) (as amended by S5959D).
[100] Dentons (n 95).
[101] New York State Assembly, 'Memorandum in Support of Legislation A5605c' <https://nyassembly.gov/leg/?Actions=Y&Chamber%252526nbspVideo%25252FTranscript=Y&Committee%252526nbspVotes=Y&Floor%252526nbspVotes=Y&Memo=Y&Summary=Y&bn=A05605&default_fld=&leg_video=&term=2019>
[102] N.Y. Civ. Rights § 50-f(2)(d)(i)-(iv) (as amended by S5959D)
[103] Dave McNary, 'SAG-AFTRA Commends Gov. Andrew Cuomo for Signing Law Banning 'Deep Fake' Videos' *Variety* (30 November 2020) <https://variety.com/2020/film/news/sag-aftra-commends-andrew-cuomo-deep-fake-videos-1234842715/>
[104] International Trademark Association, 'Right of Publicity State of the Law Survey' (2019) <https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/INTA_2019_rop_survey.pdf>
[105] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final)
[106] Article 52 'Transparency obligations for certain AI systems', Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final.
[107] This rule seems to have drawn on the Californian Bolstering Online Transparency (BOT) Act 2018.
[108] Recital 70 adds that users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin.
[109] Article 7 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16
[110] M Veale and FZ Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act', *CRi* 4/2021 at https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf.

gued that enough law already exists to protect against fraud or abuse online and that a warnings rule adds little or nothing.

5. Ways forward: 'do not bot me'

In Section 4 above, we argued that as, in principle and in most legal systems, no rights of privacy or reputation survive death, there is little chance for living persons to exert control over what is done with their data after their death. This doctrine appears, however, to be being partially eroded, given the growth in the number of countries legislating for post-mortem data protection rights for heirs. But these laws still only give rights for heirs to choose to exercise– e.g. a right to erase unpleasant publications about the deceased, as in *ML v Slovakia* – as opposed to any right to control, while alive, what happens to your data after you are dead. By contrast, it is normal to be able to control what happens to one's material property after death by devices like wills, testaments or trusts. If such a paradigm was adopted for personal data, then data subjects would be able to use such testamentary instruments to block the creation of themselves as ghostbots or perhaps be able to allocate ownership of such a ghostbot to particular legatees.

This is a 'property' framing. An alternative approach, truly based on post-mortem privacy, would be to argue that the deceased should not be compelled to 'live on' contrary to their will and desire, creating a form of 'forced immortality'. Öhman and Floridi suggest that this might violate the autonomy of the living, especially if or when their image is commercially exploited by different digital business models (the 'digital afterlife industry').[111] Another familiar factor to consider is to what extent society should allow a person to control their image and story beyond the grave if it restricts the freedoms and interests of the living; might it restrain the archiving and retelling of history as well as the creation of new forms of expression? This issue has been considered more recently in the debates around the 'right to be forgotten', and the sky does not seem to have fallen. Laws now and in the past that forbade grave robbing and desecration would lead us to think that some protection of or respect for the deceased's person is accepted.[112] What is less clear is whether that respect extends to the deceased's identity or data-self, and if so, how it should be balanced with, inter alia, the wishes and rights of living heirs, the interests of friends and family, and the public interest in truth, history and expression. It might also be argued that rules about the desecration of bodies and graves are more about the feelings and reputation of surviving family than respect for the dead. Put bluntly, is it reasonable, on the grounds of autonomy, to give a person who wants it a simple veto over some uses or abuses of their data after death?

Do we have evidence that this is something people want? Some well-known anecdotes already illustrate that some clearly want such a veto, but it is not easy to obtain: Kafka failed to secure the destruction of his unfinished works, while Pratchett did by dint of physically destroying his unfinished novel with a steamroller that crushed his hard disk.[113] More robust evidence about ordinary non-novelists has to date been thin on the ground, but research has recently shown that there is a disjunct between the wishes users express relating to what happens to their personal data after death and their general behaviour pre-mortem.[114] This has been christened the 'post-mortem privacy paradox'. Users say they want to protect or delete their data after death, but in fact, during life, they fail to avail themselves of what would help with this, the 'digital will' options on leading platforms such as Facebook and Google mentioned above.[115]

We thus argue, on the grounds of autonomy, and a shift in societal wishes, that if a deceased makes an express wish by will or another device, such as a platform 'digital will' tool, they should not be made into a ghostbot, this request should be binding and enforceable unless there is prevailing evidence of contrary public interest. We name this a 'do not bot me' clause.[116] The key issue, of course, is whether such a personal wish could be legally and practically enforced contrary to the wishes of an administrator or next of kin.[117] One solution might be to have a searchable register of such requests. If a commercial company or provider of ghostbots was commissioned to make a bot, they would have to consult the register. If they ignored a veto, civil and even criminal sanctions could apply. An approach like this could also be automated, as is indeed possible right now. If a wish for data to be deleted on death was recorded in a digital will relating to a platform like Facebook or Google, then on receipt of proof of death, the platform could automatically set deletion in motion without the need for a human administrator to be involved or have opportunity to countermand. A more detailed wish, e.g. to have the data transferred to a certain person or charity, could also, at least in theory, be implemented.[118] A problem here is that there is no formal transnational system for platforms to recog-

[111] Carl Öhman and Luciano Floridi, 'The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry' 27(4) (2017) *Minds and Machines* 639,

[112] *Burrows v HM Coroner for Preston* [2008] EWHC 1387; *Ibuna v Arroyo* [2012] EWHC 428 (Ch); for more see Heather Conway, *The Law and the Dead* (Routledge 2016), and Davey (n 63) 90 - 96.

[113] Stephanie Convery, 'Terry Pratchett's Unfinished Novels Destroyed by Steamroller' (*The Guardian*,20 August 2017) <https://www.theguardian.com/books/2017/aug/30/terry-pratchettunfinished-novels-destroyed-streamroller>; Edwards and Harbinja (n 12), 276,

[114] Morse and Birnhack (n 63).

[115] Morse and Birnhack also argue that this phenomenon takes the form of a reverse paradox as well, where the desire to share data post-mortem, is also limited by a privacy prohibitive behaviours pre-mortem, where the person protects their data and the access is disabled to those they would like to share with. Morse and Birnhack (n 63).

[116] There is recent real-life example of this. In response to another example of a Ghostbot called Re;memory, American writer, Colette Shade, tweeted 'Writing a will right now so no one can do this to me'. Colette Shade (Twitter, 10 January 2023) https://twitter.com/MsShade/status/1612675939074277378 accessed 12 February 2023.

[117] For this reason, the law currently generally makes personal wishes eg to be cremated, unenforceable in wills. See the recent case *Ilott (Respondent) v The Blue Cross and others (Appellants) [2017] UKSC 17*.

[118] Burkhard Schafer, 'On Living and Undead Wills: ZombAIs, Technology and the Future of Inheritance Law' in Lilian Edwards, Edina Harbinja and Burkhard Schafer (eds), *Future Law, Emerging Technology, Regulation and Ethics* (Edinburgh University Press 2020).

nise certificates of death across jurisdictions in any electronic and automated fashion, which would be essential to make such a scheme practical.

The European Commission has recently proposed a Declaration on European Digital Rights and Principles, which includes the interesting and somewhat surprising proposition: 'Everyone should be able to determine their digital legacy, and decide what happens with the publicly available information that concerns them, after their death.'[119] Although this declaration, even if passed, would have no binding character, it shows a remarkable shift from the norm we have chronicled in previous articles of no respect for post-mortem privacy. The hard work of translating this sentiment into enforceable legislation, alongside code for implementation on platforms, and public education, starts here.

Declaration of Competing Interest

The authors have no conflict of interest other than being co-editors of the VSI Digital Legacy.

Data availability

No data was used for the research described in the article.

Funder

This paper is a result of the "Emerging Technologies, Privacy Law and the Dead" workshop in April 2021, funded by the Modern Law Review. The workshop was facilitated by members of the Leverhulme-funded research group "Modern Technologies, Privacy Law and the Dead", grant number: RPG 2020-048.

[119] European Commission, 'European Declaration on Digital Rights and Principles for the Digital Decade', Brussels, 26.1.2022, COM(2022) 28 final, at: https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles p. 5.