



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DIGITAL RESURRECTION AND POSTHUMOUS PRIVACY: WHO OWNS YOUR DATA AFTER DEATH?

An examination of the legal, ethical, and technological dilemmas surrounding the dead in the digital age

Samikhya Patro

ABSTRACT

The rapid growth of artificial intelligence has transformed the way digital identities persist after death, giving rise to technologies capable of recreating a deceased person's voice, appearance, and manner of communication. While these developments offer new possibilities for preserving memories and supporting grieving families, they also raise complex legal and ethical questions concerning privacy, consent, ownership, dignity, and posthumous identity. This paper examines the legal status of digital assets after death through a comparative analysis of international legal frameworks, platform policies, and the existing position under Indian law. Adopting a doctrinal and comparative legal methodology¹, it explores whether traditional principles of inheritance, data protection, and personality rights are capable of addressing AI-enabled digital resurrection. The paper argues that existing legal frameworks primarily treat digital assets as inheritable property, while failing to recognise the distinct concerns associated with recreating a person's identity through artificial intelligence. It concludes that regulating digital resurrection requires a framework centred on informed consent, posthumous dignity, and responsible technological

¹ Terry Hutchinson & Nigel Duncan, Defining and Describing What We Do: Doctrinal Legal Research, 17 Deakin L. Rev. 83 (2012).

governance rather than conventional property-based approaches. By highlighting the growing gap between technological capability and legal regulation, the paper advocates for a more coherent legal response to protect both the interests of the deceased and the rights of those who survive them.

KEYWORDS: Digital Resurrection; Artificial Intelligence; Posthumous Privacy; Digital Assets; Digital Legacy; Consent; Data Protection.

1. INTRODUCTION

In 2020, a South Korean documentary crew used motion capture and voice synthesis to let a grieving mother speak with a virtual reconstruction of her deceased daughter in a virtual reality headset². The footage went viral, and reactions split sharply between those who found it a moving form of closure and those who found it deeply disturbing, an act that treated grief as raw material for content. That split reaction is the entire subject of this paper in miniature. We are no longer simply asking who gets access to a dead relative's email account or Facebook page. We are asking whether a company, a family member, or even a stranger should be allowed to construct a working simulation of someone who can no longer consent, object, or correct the record.

The term commonly used for this practice is digital resurrection, sometimes called griefbots, deadbots, or digital afterlife services³. The underlying technology is not exotic. Large language models can be fine-tuned⁴ on a person's text messages, emails, and social media history to produce a chatbot that writes in their voice. Voice cloning tools need only a few minutes of audio to generate new sentences in a recognisable timbre. Video synthesis can animate a still photograph to nod, blink, and speak. None of these capabilities are restricted to research labs anymore; several commercial apps already let ordinary users feed in a deceased relative's messages and receive a chatbot in return, usually marketed as a grief support tool.

This paper has three goals. First, to map the existing legal terrain that governs digital assets after death, since that terrain is the foundation on which any resurrection technology necessarily stands.

² Munhwa Broadcasting Corp. (MBC), *Meeting You* (2020).

³ Carl Öhman & Luciano Floridi, *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*, 23 *Minds & Machines* 639 (2018).

⁴ Luciano Floridi, *The Ethics of Information* (Oxford Univ. Press 2013).

Second, to examine how technology platforms have responded, often inconsistently, to requests from grieving families. Third, and most importantly, to argue that ownership and consent are not the same question, and that current law is much better equipped to answer the first than the second.

RESEARCH METHODOLOGY

This paper adopts a doctrinal and comparative legal methodology. It examines statutes, judicial decisions, platform policies, and academic scholarship from multiple jurisdictions to analyse the legal challenges posed by digital resurrection and posthumous data governance. Since no comprehensive legal framework presently exists for AI-enabled digital resurrection, the discussion also draws upon ethical literature and emerging regulatory developments to evaluate whether existing legal principles relating to privacy, inheritance, consent, and personality rights are capable of addressing these new technological realities.

2. THE LEGAL STATUS OF DIGITAL ASSETS AFTER DEATH

Most legal systems were not designed with digital assets in mind, and the result is a body of law assembled from borrowed concepts. In the United States, the primary statutory tool is the Revised Uniform Fiduciary Access to Digital Assets Act⁵, adopted in some form by nearly every state. The Act allows a person to designate, through a will or an online tool, who should have access to their digital accounts after death. Where no designation exists, the platform's terms of service typically take precedence⁶ over a family member's wishes, which is why a grieving spouse can find themselves locked out of a deceased partner's email account despite knowing the password.

The European approach differs in an important way because of the General Data Protection Regulation⁷. The GDPR explicitly defines personal data as information relating to a living individual, which means the dead fall outside its protective scope in most member states. A handful of countries, including France, have layered their own posthumous data protection rules on top of this gap, giving individuals the right to leave binding instructions about what should happen to their data after death, comparable to a digital will⁸. Germany has gone further still through court

⁵ Revised Uniform Fiduciary Access to Digital Assets Act (Unif. L. Comm'n 2015).

⁶ Naomi Cahn, *Probate Law Meets the Digital Age*, 67 Vand. L. Rev. 1697 (2014).

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, as amended.

precedent, ruling in a widely discussed case that a deceased person's social media account should be treated like any other inheritable asset, accessible to heirs in the same way a paper diary would be.⁹

The position in India remains considerably less developed. While the Digital Personal Data Protection Act, 2023¹⁰ establishes a comprehensive framework for the protection and processing of personal data, its protection is limited to living individuals and does not expressly address the legal status of personal data after death. Likewise, the Information Technology Act, 2000¹¹ regulates electronic records, cyber offences, and intermediary liability but contains no provisions governing posthumous digital identities or AI-assisted recreations of deceased persons. As a result, Indian law offers little guidance on whether a deceased individual's digital footprint may be inherited, accessed, or repurposed to generate synthetic versions of their personality.

The absence of a dedicated legal framework is particularly significant in light of the Supreme Court's recognition of privacy as a fundamental right in *Justice K. S. Puttaswamy (Retd.) v. Union of India*¹². Although the judgment speaks in the context of living individuals, its emphasis on dignity, autonomy, and informational self-determination raises broader questions about whether these values should continue to influence the treatment of a person's digital identity after death. At present, Indian law leaves these questions unanswered, creating uncertainty for families, technology companies, and courts alike.¹³

The comparative legal position across major jurisdictions demonstrates that while several countries have introduced mechanisms governing access to digital assets after death, very few have specifically addressed AI-enabled digital resurrection. The position is summarised in Table 1 below.

⁹ Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2018, III ZR 183/17 (Ger.).

¹⁰ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

¹¹ Information Technology Act, No. 21 of 2000, India Code (2000).

¹² *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹³ Edina Harbinja, *Post-Mortem Privacy 2.0: Theory, Law and Technology*, 31 Int'l Rev. L. Computers & Tech. 26 (2017).

TABLE 1
**COMPARATIVE LEGAL POSITION ON POSTHUMOUS DIGITAL ASSETS AND AI-
 ENABLED DIGITAL RESURRECTION**

Jurisdiction	Posthumous Digital Assets	AI Digital Resurrection
India	No dedicated legal framework	No specific regulation
United States	RUFADAA permits fiduciary access	Fragmented state-level protection
European Union	GDPR generally excludes deceased persons	No harmonised framework
France	Posthumous digital directives recognised	Limited regulation
Germany	Digital accounts treated as inheritable	No specific AI legislation

As Table 1 illustrates, existing legal frameworks primarily regulate inheritance or access to digital assets, whereas AI-generated posthumous identities remain largely unregulated. This common gap underscores the need for a legal framework that distinguishes between ownership of digital assets and the creation of synthetic digital identities.

What unites these frameworks is a shared assumption that digital remains are best understood through the language of property and inheritance. That assumption works reasonably well for static data: an email archive, a photo library, a list of online subscriptions. It becomes far less satisfying once the data in question can be reassembled into something that talks back. A property framework asks who gets to keep the photo album. It has very little to say about whether someone should be allowed to use that album to build a talking avatar of the person in it.

3. PLATFORM POLICIES AND THEIR LIMITS

Major technology companies have each developed their own posthumous policies, and the variation between them illustrates how unsettled this area remains. Facebook, now under Meta, allows accounts to be converted into memorialised profiles¹⁴, frozen in place with the word Remembering displayed above the name, and it permits a designated legacy contact to manage limited aspects of the page. Unlike statutory frameworks enacted by legislatures, these policies operate as contractual arrangements between users and private platforms, resulting in significant differences in how digital assets are managed after death. Google offers an Inactive Account Manager, letting users decide in advance whether their data should be deleted or shared with a trusted contact after a period of inactivity¹⁵. Apple introduced a Legacy Contact feature that grants a nominated person access to photos, messages, and files stored in iCloud upon presentation of a death certificate.¹⁶

The rapid emergence of generative AI has also shifted attention towards companies that specialise in conversational AI and voice synthesis rather than traditional technology platforms alone. Services capable of producing realistic voice clones or AI companions increasingly make it possible to recreate aspects of a deceased person's identity using previously shared digital content. Despite the growing accessibility of these technologies, few providers have adopted detailed policies governing the posthumous use of personal data or established mechanisms for verifying whether the deceased had consented to such recreation during their lifetime. This regulatory silence reflects the speed with which technological innovation has outpaced legal and institutional responses.¹⁷

These policies share a quiet limitation: they govern access to existing data, not the creation of new synthetic content derived from it. A legacy contact who gains access to a deceased person's photo library is not thereby authorised, under any platform's current terms, to feed those photos into an AI tool and generate new video footage of the person saying things they never said. That gap exists

¹⁴ Meta Platforms, Inc., Memorialization Settings, <https://www.facebook.com/help/1506822589577997> (last visited July 1, 2026).

¹⁵ Google, Inactive Account Manager, <https://support.google.com/accounts/answer/3036546> (last visited July 1, 2026).

¹⁶ Apple Inc., How to Add a Legacy Contact for Your Apple Account, <https://support.apple.com/en-us/102631> (last visited July 1, 2026).

¹⁷ OpenAI, *GPT-4 Technical Report* (2023); ElevenLabs, Safety & AI Voice Technology, available on the company's official website.

because the policies were written before generative AI made such reconstruction trivial, and few companies have updated their terms to address it directly. The result is a legal vacuum in which the technical capability has outpaced the governing rules by several years.¹⁸

Some platforms have begun reacting to specific controversies rather than building comprehensive policy in advance. After public unease about AI-generated tribute videos using a deceased celebrity's likeness without estate approval, several jurisdictions have moved to strengthen postmortem rights of publicity, the legal doctrine that controls commercial use of a person's name, image, and voice. Tennessee's ELVIS Act, passed in 2024 and named with a wink toward Elvis Presley, specifically extends these protections to voice cloning, making it one of the first statutes to explicitly contemplate AI-driven resurrection of a person's persona¹⁹. Such laws are promising but narrow, generally protecting commercial exploitation while leaving private, non-commercial recreation by grieving family members largely untouched.²⁰

4. DIGITAL RESURRECTION AS A DISTINCT ETHICAL PROBLEM

It helps to separate two questions that are often blurred together. The first is a question of ownership: who has the legal right to control a dead person's data. The second is a question of personhood: whether reconstructing a simulacrum of someone violates something about their dignity that survives their death, independent of who technically owns the underlying files. Most existing law answers only the first question, yet most of the public discomfort with digital resurrection clearly stems from the second.²¹

Philosophers writing on posthumous harm have long debated whether the dead can be wronged at all²², given that they no longer exist to experience the wrong. One influential line of reasoning, associated with thinkers in the Epicurean tradition, holds that death removes the subject capable of being harmed, so nothing done afterward can hurt them²³. A competing view argues that

¹⁸ Carl Öhman, Digital Remains: The Social and Ethical Implications of Digitally Extended Lives, in *The Oxford Handbook of Digital Ethics* (2023).

¹⁹ Ensuring Likeness, Voice, and Image Security (ELVIS) Act, Tenn. Code Ann. § 47-25-1101 (2024).

²⁰ Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* (Harvard Univ. Press 2018).

²¹ Luciano Floridi & Carl Öhman, The Ethics of Information and the Digital Afterlife, 23 *Minds & Machines* 639 (2018).

²² Joel Feinberg, Harm to Others, in *The Moral Limits of the Criminal Law* 79 (1984).

²³ Epicurus, *Letter to Menoeceus*, in *The Epicurus Reader* (Brad Inwood & L. P. Gerson eds., 1994).

interests can outlive the interest-holder in a meaningful sense, in the same way that a person's wish to have their novel published posthumously, or their reputation protected from defamation, retains moral weight²⁴ even though they are not present to feel the benefit or the injury. Digital resurrection sits squarely in this unresolved philosophical territory²⁵, because a chatbot built from someone's old messages does not merely store their words, it generates new ones, attributed to a person who never approved them and cannot revise them.

This is the crux of the consent problem. Even a person who was perfectly comfortable sharing photos and messages during their lifetime may never have anticipated, let alone consented to, those materials being used to train a model that produces novel statements in their name. Consent given for one purpose, ordinary social communication, is being silently repurposed for another, synthetic continuation. Few terms of service from a decade ago, when most of this data was originally generated, even mention the possibility of AI training, which means the consent on record is almost always retroactively stretched rather than freely given.²⁶

The issue also extends beyond consent to the broader concept of identity. A digital recreation does not simply preserve a person's past expressions; it actively generates new conversations, opinions, and responses that never existed during the individual's lifetime. Over time, these generated interactions may gradually reshape how future generations remember the deceased, blurring the distinction between authentic memory and algorithmic reconstruction. In this sense, digital resurrection has the potential not only to preserve identity but also to rewrite it, raising profound concerns about authenticity and historical truth.²⁷

There is also a real risk to the grieving family itself, separate from any harm to the deceased. Researchers studying prolonged and complicated grief have raised concerns that ongoing interaction with a deadbot may interfere with the natural process of acceptance²⁸, allowing a person to defer the emotional work of mourning by maintaining a simulated relationship instead. A chatbot that responds instantly, agreeably, and indefinitely is a very different object than a

²⁴ Joel Feinberg, *The Rights of Animals and Unborn Generations*, in *Rights, Justice, and the Bounds of Liberty* (1980).

²⁵ Lilian Edwards & Edina Harbinja, *Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World*, 32 Cardozo Arts & Ent. L.J. 83 (2014).

²⁶ Luciano Floridi, *The Ethics of Information* (Oxford Univ. Press 2013).

²⁷ Shannon Vallor, *Technology and the Virtues* (Oxford Univ. Press 2016).

²⁸ Elaine Kasket, *All the Ghosts in the Machine: Illusions of Immortality in the Digital Age* (Robinson 2019).

memory, which fades, contradicts itself, and eventually settles into something the living person can carry forward. Some early qualitative studies of users interacting with griefbots describe a sense of comfort in the first weeks followed by a creeping unease, a feeling that the technology offers an artificial steadiness that real relationships, even remembered ones, never had.²⁹

Children raise a sharper version of this dilemma. A young child who loses a parent and is given a chatbot version of that parent to talk to may not have the cognitive tools to understand that the responses are statistically generated rather than authentically remembered. The long-term psychological effects of growing up with a simulated parent, rather than grieving an absent one, are entirely unstudied, since the technology enabling this is only a few years old. Regulatory frameworks built around adult autonomy and informed consent are particularly weak tools for governing a scenario where the most affected party, the child, has no meaningful capacity to consent at all.³⁰

5. COMMERCIAL INCENTIVES AND THE RISK OF EXPLOITATION

It would be naive to treat digital afterlife services purely as acts of compassion. Several startups in this space operate on subscription models, meaning a grieving customer pays monthly to keep talking to a simulated version of a dead relative.³¹ This creates a financial incentive structure that rewards prolonged engagement rather than healthy closure, the same dynamic that critics have long raised about social media more broadly, now applied to one of the most emotionally vulnerable moments a person can experience³². A company whose revenue depends on a widow continuing to message her late husband's chatbot has little structural incentive to encourage her toward the kind of acceptance that would lead her to stop using the product.

There is also the question of what happens to the data these services collect. A person grieving a parent who shares old voice memos, private letters, and intimate family history with an AI resurrection company is handing over material that is, by definition, irreplaceable and impossible to consent to on behalf of the deceased. If that company is later acquired, breached, or simply

²⁹ Elaine Kasket, *All the Ghosts in the Machine: Illusions of Immortality in the Digital Age* (Robinson 2019).

³⁰ United Nations Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

³¹ Carl Öhman, *The Afterlife of Data: What Happens to Your Information When You Die and Why You Should Care*, 22 Internet Pol'y Rev. (2023).

³² Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

changes its data practices, the family has effectively lost control over the most sensitive archive of a loved one's life, often with no clear legal remedy, since the deceased was never a party to any contract and the living relative's standing to object varies enormously by jurisdiction.

Questions surrounding intellectual property further complicate this landscape. If an artificial intelligence system generates entirely new conversations in the style of a deceased individual, uncertainty arises regarding ownership of that output. The underlying data may belong to the deceased, the lawful heirs may possess access rights, and the AI company may claim rights over the generated content under its terms of service. Existing copyright and personality-rights doctrines were not developed with such layered claims in mind, leaving significant ambiguity regarding who may commercially exploit AI-generated representations of the dead.³³

6. TOWARD A WORKABLE FRAMEWORK

None of this argues that digital resurrection should be banned outright. There are documented cases of therapeutic value, particularly in carefully supervised clinical contexts where a temporary, professionally guided interaction with a simulated voice has helped a person process specific unresolved conversations. The goal should not be prohibition but structure, built around three principles that current law largely ignores.

The first principle is anticipatory consent. Just as a person can specify organ donation preferences or write a living will, platforms and lawmakers should create a clear, accessible mechanism for individuals to state, while alive, whether they consent to their data being used for AI recreation after death, and if so, under what limits. A handful of jurisdictions are experimenting with exactly this through expanded digital will provisions³⁴, and the approach deserves wider adoption rather than remaining a niche legal curiosity.

The second principle is purpose limitation specific to synthetic generation. Existing inheritance and access laws were written for static retrieval, not generative reuse³⁵, and that gap needs to be closed explicitly. A legacy contact's authority to view a photo library should not automatically

³³ Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* (Harvard Univ. Press 2018).

³⁴ Council of Europe, Recommendation CM/Rec(2019)2 on the Protection of Health-Related Data (illustrating advance consent principles); see also French Data Protection Act (digital directives provisions).

³⁵ Regulation (EU) 2016/679 (General Data Protection Regulation), art. 5(1)(b) (purpose limitation principle).

extend to authority for using that library as AI training data, and law should say so directly rather than leaving the question to be inferred from terms of service written for a different technological era.

The third principle is time-boxing and transparency for any deadbot product that does operate, whether through clinical or commercial channels. Users interacting with a digital recreation should be reminded, clearly and repeatedly rather than buried in a one-time disclaimer, that they are speaking with a statistical model and not a continuation of the person³⁶. Indefinite, unsupervised use should be discouraged by design, with services structured to taper off rather than maximise engagement, a sharp departure from the incentives that currently shape most consumer software.

Underlying all three principles is a single conceptual shift that the law has yet to make: digital remains are not simply property to be inherited³⁷, distributed, or licensed. They are residue of a person, and decisions about how that residue is used after death deserve a framework closer to medical ethics, with its emphasis on consent, dignity, and the limits of what can be done to a person who cannot object, than to estate law, with its emphasis on efficient transfer of assets.

While these three principles provide an important foundation, they are not sufficient on their own to address the broader legal challenges posed by digital resurrection. A more comprehensive regulatory framework must distinguish between access to digital assets and the creation of AI-generated identities. While inheritance laws may appropriately govern the transfer of emails, photographs, and online accounts, the generation of new speech or behaviour through artificial intelligence raises distinct concerns that warrant independent legal safeguards. Legislatures should therefore recognise posthumous digital identity as a separate legal interest³⁸ rather than treating it as an ordinary component of inherited property.

Such a framework should also establish clear obligations for technology companies. Providers offering digital resurrection services should verify documented consent from the deceased wherever reasonably possible, maintain transparency regarding the artificial nature of all interactions, prohibit deceptive representations that suggest genuine consciousness or continued

³⁶ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

³⁷ Carl Öhman, *Data and the Afterlife*, in *The Oxford Handbook of Digital Ethics* (Carissa Véliz ed., Oxford Univ. Press 2023).

³⁸ Luciano Floridi, *The Ethics of Information* (Oxford Univ. Press 2013).

existence, and implement enhanced safeguards where minors or vulnerable individuals are involved. Rather than restricting innovation altogether, regulation should ensure that technological advancement remains consistent with the principles of dignity, informed consent, transparency, and accountability. Such an approach would encourage responsible innovation while safeguarding the interests of both the deceased and their surviving families.³⁹

FUTURE CHALLENGES

The legal questions surrounding digital resurrection are likely to become more complex as artificial intelligence systems continue to improve. Advances in multimodal models capable of simultaneously replicating a person's voice, appearance, mannerisms, and conversational style may soon produce digital recreations that are increasingly indistinguishable from authentic human interaction. Existing legal categories of privacy, succession, copyright, and personality rights were developed for a world in which death marked the end of active participation in society. As that assumption becomes technologically unstable, future legislation will need to balance innovation with the preservation of dignity, autonomy, and public trust.

7. CONCLUSION

The question posed at the outset—who owns a person's data after death—cannot be answered by the law of property alone. As this paper has demonstrated, digital resurrection presents challenges that extend beyond ownership into questions of privacy, consent, dignity, and the continued protection of personal identity. Existing legal frameworks, whether based on inheritance, data protection, or platform governance, provide limited guidance for technologies capable of recreating a deceased person's voice, appearance, and manner of communication through artificial intelligence.

The comparative analysis further reveals that while several jurisdictions have taken initial steps to regulate posthumous digital assets, none offers a comprehensive legal framework specifically addressing AI-enabled digital resurrection. The position in India remains particularly uncertain, as existing legislation does not expressly regulate the creation or use of digital identities after death.

³⁹ OECD, *OECD AI Principles* (2019); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

This legal gap becomes increasingly significant as generative AI technologies become more sophisticated, accessible, and commercially viable.

The paper has argued that regulating digital resurrection requires a shift in legal thinking. Digital remains should not be viewed merely as inheritable property but as an extension of an individual's identity that continues to raise questions of autonomy and dignity even after death. Any future regulatory framework should therefore distinguish between access to digital assets and the creation of AI-generated identities, while placing informed consent, transparency, and accountability at the centre of legal governance.

Ultimately, digital resurrection represents one of the most significant intersections between artificial intelligence, privacy, and human dignity. The challenge before lawmakers is not simply to determine who owns digital data after death, but to decide how society should protect the memory, identity, and dignity of those who are no longer able to speak for themselves. As technological capability continues to advance, the law must evolve with equal urgency to ensure that innovation serves humanity without compromising the values that define it.

REFERENCES

A. Legislation

- Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
- Information Technology Act, No. 21 of 2000, India Code (2000).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Revised Uniform Fiduciary Access to Digital Assets Act (Unif. L. Comm'n 2015).
- Ensuring Likeness, Voice, and Image Security (ELVIS) Act, Tenn. Code Ann. § 47-25-1101 (2024).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (France).

B. Cases

- Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2018, III ZR 183/17 (Ger.).
- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

C. Books

- Feinberg, Joel. *Harm to Others*. Oxford University Press, 1984.
- Floridi, Luciano. *The Ethics of Information*. Oxford University Press, 2013.
- Kasket, Elaine. *All the Ghosts in the Machine: Illusions of Immortality in the Digital Age*. Robinson, 2019.
- Rothman, Jennifer E. *The Right of Publicity: Privacy Reimagined for a Public World*. Harvard University Press, 2018.
- Vallor, Shannon. *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. Oxford University Press, 2016.

- Zuboff, Shoshana. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.

D. Journal Articles

- Hutchinson, Terry & Nigel Duncan. "Defining and Describing What We Do: Doctrinal Legal Research." *Deakin Law Review* 17 (2012): 83–119.
- Öhman, Carl & Luciano Floridi. "The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry." *Minds and Machines* 28 (2018): 639–662.
- Cahn, Naomi. "Probate Law Meets the Digital Age." *Vanderbilt Law Review* 67 (2014): 1697–1734.
- Edwards, Lilian & Edina Harbinja. "Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World." *Cardozo Arts & Entertainment Law Journal* 32 (2014): 83–129.
- Harbinja, Edina. "Post-Mortem Privacy 2.0: Theory, Law and Technology." *International Review of Law, Computers & Technology* 31 (2017): 26–42.

E. Reports and Policy Documents

- Google. *Inactive Account Manager*. <https://support.google.com/accounts/answer/3036546>
- Meta Platforms, Inc. *Memorialization Settings*. <https://www.facebook.com/help/1506822589577997>
- Apple Inc. *Legacy Contact for Apple Account*. <https://support.apple.com/>
- OECD. *OECD Principles on Artificial Intelligence*. 2019.
- UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. 2021.
- European Parliamentary Research Service. *Artificial Intelligence and the Digital Transformation of Society*. 2020.
- Munhwa Broadcasting Corporation (MBC). *Meeting You*. 2020.

