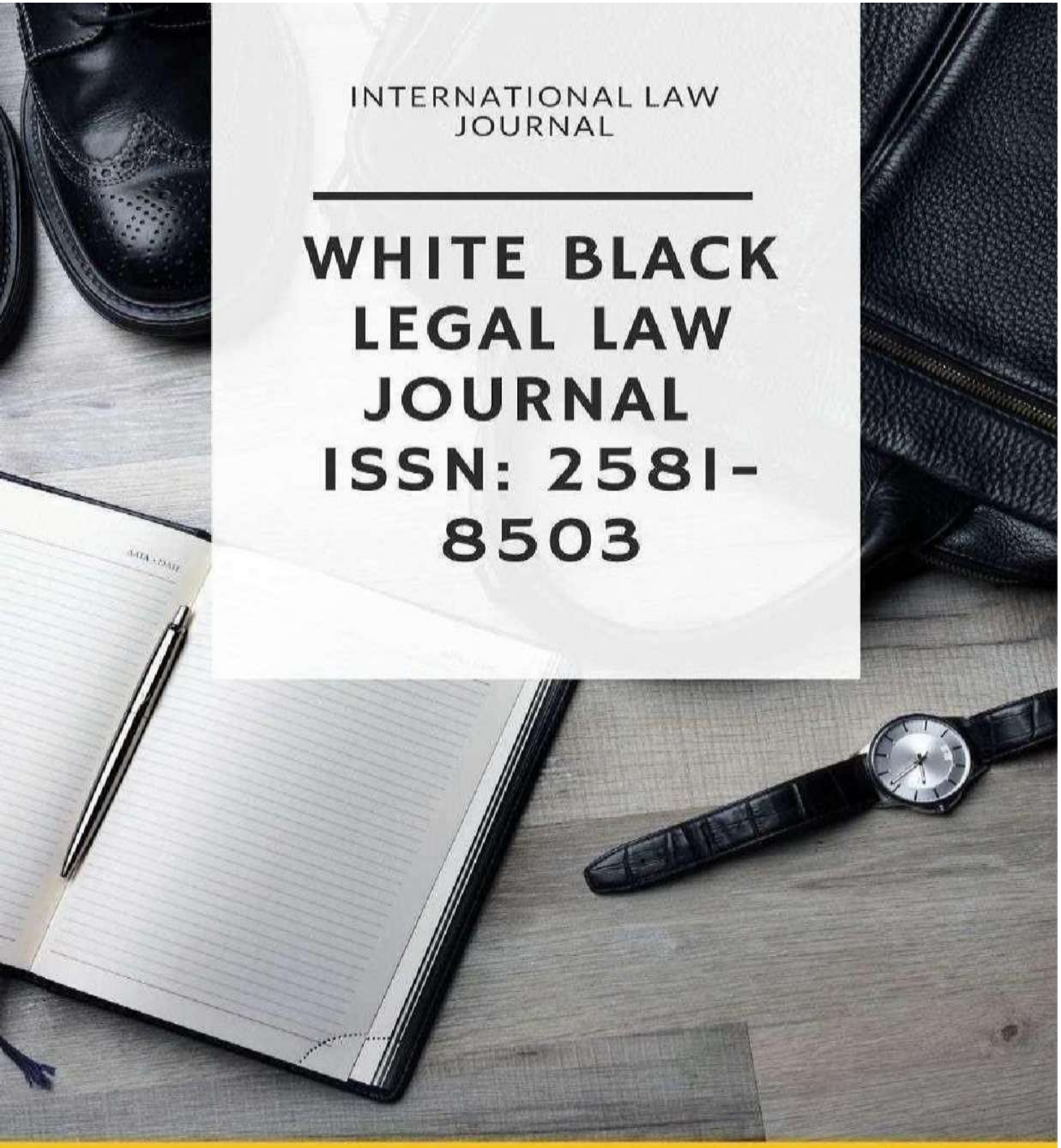

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

FROM MEMORIALIZATION TO MANIPULATION: LEGAL REGULATION OF POSTHUMOUS DIGITAL IDENTITIES IN INDIA

AUTHORED BY - STEVE BENNETT

Class: 5 BBA LLB

3rd year Student at School of Law,

CHRIST (Deemed to be University), Pune Lavasa Campus

Abstract

Digital life does not cease with the body[1]. Our online footprints messages, images, social media accounts, digital currencies, and even AI trained on our words linger, shape memory, and occasionally cause genuine harm to the living[2]. This article brings together key scholarship, case studies, and comparative law to investigate how India might shift from ad hoc platform practices and obsolete rules toward a coherent strategy that respects dignity, prevents abuse, and helps families and people to plan for their digital legacies.The present legal mechanisms, from succession law to data protection regulations, were developed for physical property and living humans[3]. They struggle to answer obvious questions: who controls a deceased person's email, who may profit from a recreated voice, and how do we balance public interest with the grief caused by misuse? Platform regulations and service agreements too often decide these results, and they rarely represent users' wants or social norms. Empirical investigations and real life occurrences demonstrate a continuous pattern[4]. People care strongly about what happens to their private data after death, yet they rarely plan for it. Strong security standards throughout life often make legitimate access after death impossible. Emerging technologies like AI and deepfakes increase urgency by making misuse cheaper and more damaging. Drawing on comparative law and technical proposals, the article advocates for a tiered response. Legal change should clarify inheritance and dignity rights for digital remains while giving people simple methods to communicate their postmortem wishes. Regulators and platforms should set transparent default policies that prioritize consent and family interests and implement technology safeguards such as selective deletion, designated legacy stewards, and machine level unlearning for sensitive data. Above all, policy must regard digital death as both a legal concern and a human one. By prioritizing dignity, predictability, and choice, India can protect the living and commemorate the dead in the age of constant digital presence.

Keywords: Digital rights, India, Posthumous identity, Memorialization, Data manipulation, Data privacy, Digital legacy.

[1] See Carl Öhman & Luciano Floridi, *The Political Economy of Death in the Age of Information*, 23 Minds & Machines 1, 3–5 (2017).
[2] 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, 86–89 (2014).
[3] Edina Harbinja, *What Happens to My Facebook Profile When I Die?*, 23 Info. & Commc'ns Tech. L. 1, 4–6 (2017).
[4] Jed R. Brubaker et al., *The Postmortem Privacy Paradox*, 17 Human-Computer Interaction 1, 4–7 (2019).

INTRODUCTION

Today's world a person's digital imprint their emails social media posts, cloud data, digital art, Cryptocurrency holdings, biometric identifiers, and even AI models trained on their content does not vanish with physical death. As researchers stress, "death is no longer a clear cut end" In the digital arena; one's online existence can "outlive the individual". These permanent traces impact how the deceased are remembered and mourned but they also provide new channels for misuse identity theft, impersonation, deepfakes scams and financial fraud targeting bereaved relatives. Surveys demonstrate enormous public anxiety, A recent Kaspersky study found 61% of respondents believe deceased individuals identities are especially vulnerable to theft and 63% think people should specify in their wills what happens to their data and account in other words while the deceased themselves cannot suffer their surviving relatives and society at large can be emotionally and materially affected if digital remains are mistreated[5].

In India with over a billion Internet users the digital afterlife presents significant questions Yet present legislation offers no direction families often find themselves locked out of the very digital arches that could help with mooring, such as photo albums or farewell messages[6]. Platforms like Facebook Google and Twitter have added ad hoc memorialization capabilities and legacy contacts, although standards varied widely and often favor the platforms control. Meanwhile, New technologies like AI chat box, speech synthesis and deepfake videos make posthumous identity reconstruction easier than ever blurring the border between remembering and exploitation. Without clear regulations, our society risks misuse of the dead's likeness for profit or fraud, Chilling effects on privacy and dignity and misunderstanding over who has the right to speak for or about someone who has passed away. This article proposes that India must alter its legal structure to acknowledge the rights of individuals after death to some degree, providing predictable rules for succession of digital assets and strong safeguards against their exploitation. It begins by dissecting the concept of the digital afterlife and attendant privacy considerations It then evaluates worldwide approaches (from EU and US data protection to publicity rights regulations) And surveys Indian legal scholarship emphasizing shortcomings It investigates how platform agreements often serve as de facto law in this arena and surveys the real world concerns from utilizing facebook profiles as memorials to criminal deepfake

[5] Kaspersky, *Digital Afterlife: Survey on Posthumous Data and Identity Theft* (2022).
[6] Internet & Mobile Ass'n of India, *Digital India: Internet User Statistics* (2023).

frauds[7]. Based on this the paper proposes a coherent regulatory model; One that treats the deceased's digital identity as a legitimate subject of law akin to a kind of inherited property or personality right, ensures families have a statutory route to access or delete data and protect the death's memory from technological manipulation. By striking a balance among personal dignity innovation and familial interests India can proceed "From memorialization to manipulation" under legislation, rather than by each platform's whim.

CONCEPTUAL FOUNDATIONS

The digital afterlife signifies the continuous existence and social effect of human data after death, covering social media accounts photo and video archives, emails and messages, cloud storage, Subscriptions, cryptocurrency wallets, NFTs, gaming avatar, and even biometric or genetic data[8]. Almost everyone builds such a legacy each post, post or email contributes to a posthuman footprint and current technologies often produce AI enhanced chat bots or holograms educated on a person's data. Families regularly use memorial pages or voice recordings to preserve memory and these virtual relics can hold emotional and sometimes economic worth (For instance, an online shop or unsent manuscripts). India already exhibits hints of this shift: tales of "Virtual funerals" And digital powers of attorney emerge[9], and forecasts (e.g., by the Oxford Internet Institute) Forsee memorialized social Accounts significantly outnumbering living uses by 2100. Despite this, Indian law does not yet treat digital data as property or inheritance saving column commentators know that existing roles "fail to explicitly address digital property inheritance" leaving cryptocurrencies email archives and profiles in legal limbo and forcing courts and courts to navigate an unclear landscape posthumous privacy. Although the departed cannot sense guilt, their personal data can profoundly affect survivors; Posthumous privacy consequently attempts to safeguard reputation secrets and dignity after death. Families can be emotionally affected if intimate images, text or medical records are disclosed or exploited. Empirical work indicates a "posthumous privacy paradox" most people say they worry about how their data is handled after death, yet few make provisions such as digital wills Surveys suggest many individuals abhor the thought of AI copies of the death yet only a few employee legacy planning tools even

[7] See generally Revised Uniform Fiduciary Access to Digital Assets Act (2015); Digital Personal Data Protection Act, No. 22 of 2023 (India).
[8] Carl Öhman & Luciano Floridi, *The Political Economy of Death in the Age of Information*, 23 Minds & Machines 1, 2–4 (2017).
[9] Orla Lynskey, *The Foundations of EU Data Protection Law* 207–09 (2015).

without ability to agree, respecting the deceased's expected preferences "Continuing privacy" is often viewed as an ethical duty rooted in familial and cultural respect. Digital manipulation and identity theft. The digital afterlife also invites exploitation Thieves can steal accounts or biometric data for fraud, clone voices with AI to extort money, or set up false memorial fundraisers to Swindle grieving. AI driven deepfakes can make convincing posthumous voice or video without family agreement Scholars distinguish unauthorized deepfakes from authorized "legacy avatars" created with consent; the former are especially hazardous because the subject cannot validate or revoke use facilitating identity theft or emotional abuse such as chat box impersonating a late partner thereby turning memorial concerns into tangible emotions and financial harms.

LITERATURE REVIEW

Global perspectives. In the lack of domestic rules, foreign countries often varied models the EU's GDPR has a strong privacy policy but excludes the deceased, but certain nations (e.g., France) Authorized Digital Death Directives the U.S. offers a patchwork many states enacted RUFADAA to provide fiduciaries access to digital assets unless users opt out, but many jurisdictions acknowledge posthumous publicity rights (e.g., California extends publicity rights 70 years). Outside the West countries differ South Koreas PIPA may indirectly Preserve deceased data without specific restriction; in Chinas PIPL concentrates on living persons and allows has minimal control; areas of Latin America treat digital assets in inheritance[10]. International bodies (e.g., the European Law Institute) are working on unifying succession of digital assets recommendations. Compared to these experiments, India has adopted leaving data in legal limbo.

INDIAN SCHOLARSHIP

Indian analysts emphasize a large statutory doctrinal difference the IT Act 2000 was drafted before social media and AI and addresses infractions against live persons; the DPDP Act 2023 similarly establishes right for living "data principles"[11]. Courts have usually considered privacy and personality rights as extinguished on death recent Delhi High Court rulings and other precedents confirm the assumption that such rights do not survive hence estate and publicity

[10] Personal Information Protection Act (S. Kor.); Personal Information Protection Law (China, 2021).
[11] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 181–84 (2018).

safeguards are weak or absent[12]. Succession laws (Indian Succession Act Hindu Succession Act, etc.) were designed around tangible property and do not specifically cover emails, social accounts, crypto or digital works; few wills list digital assets and there is no settled procedure for valuation or transfer[13]. As a result, digital accounts are generally controlled by platform contracts rather than estate law forcing hires and executors to navigate contradictory conditions and probable laws or misappropriation. Platform governance in effect large platforms function as de facto regulators by enforcing non transferability provisions and different memorialization methods Yahoo historically reserved rights to terminate accounts on death; google offers an inactive account manager but access often requires prior user setup; Facebook provides memorialization and legacy contracts but only if designated; twitter/X generally deactivates on request without granting Hier access. Heirs frequently must submit death certificates and seek individual petitions and high-profile outliners (like the Ellsworth email case in the U.S.) demonstrate quotes can override platform TOS but such rulings are unusual and jurisdiction specific. Critics warn platforms may monetize deceased users' content or used to train algorithms, effectively creating the dead "data subjects without rates". The absence of legislative limits leaves ethical problems unaddressed and cedes de facto control of legacy to corporate policies.

COMPARITIVE ANALYSIS

Consequently, India presently lacks a definitive framework for managing the digital legacies of its residents. Certain nations regard digital assets as comparable to inheritable property; Are those classified the best personal data subject to privacy safeguards (or lack thereof), while some emphasize personality or publicity rights will stop the Uks Property Digital Assets etc act 2025 specifically established that crypto assets and other digital rights are recognized as property concerning ownership and inheritance Consequently combine the UK, these digital assets will be incorporated into an individual's estate and distributed akin to monetary assets or jewelry[14]. The United States has a hybrid strategy Certain data is proprietary, others A personal, and platforms frequently exert dominance through contractual agreements. The EU's approach is multifaceted; GDPR does not extend protections to the deceased, although EU policy talks advocate for data minimization and user permission come up with some nations

[12] Krishna Kishore Singh v. Sarla A. Saraogi, (2021) 4 S.C.C. 307 (India); Ruba Ahmed v. Hansal Mehta, 2022 SCC OnLine Del 164.
[13] Arpita Mitra, *Digital Assets and Succession Law in India*, 45 Econ. & Pol. Wkly. 62, 64–66 (2023).
[14] U.K. Law Commission, *Digital Assets: Consultation Paper* 2.45–2.52 (2023).

permitting persons to provide directives[15]. Chinas legislation prioritizes individual data rights, specifically pertaining to living individual. Low global standard has emerged. Currently, India lags in this initiative, as its legislation has not definitely classified digital remains as property, data or personhood This comparative vacuum shows that India is free to forge its own course preferably guided by successful elements overseas but also highlights the urgency that something must be done, lest it become an outlier with no guidance. Platform terms of service as de facto law.

CONTRACTUAL OVERREACH

In Actuality the destiny of most digital accounts after death is established by private contracts particularly user agreements. Every major digital platform includes terms saying that user accounts are non-transferable and expire on death. For instance, Yahoo's terms simply stated, "Your account is non-transferable and any rights to your Yahoo! ID or content terminate upon your death," and it explicitly reserved the right to deactivate the account whenever given a death certificateillinoisattorneyblog.blogspot.com. Facebook's policy also needs proof of death to even commemorate or deactivate an account, but otherwise grants no inheritance rights to heirs. Twitter (X) only enables post-death deactivation, not access[16]. In fact, these contracts override Indian succession principles. Heirs who might have valid claims (say, to family photos or key communications) find themselves prohibited by the "fine print" they never discussed. Indeed, the irony is striking: a user may die thinking their loved ones can access beloved memories, only for the TOS to declare the reverse. One legal observer argues that platforms have become "de facto lawmakers," since end-users seldom read or have any negotiation authority over these rules.

Case Studies. The most notable illustration is the Ellsworth case in the U.S. (Mich. 2010)[17], where a marine's parents fought Yahoo for his emails. Yahoo first denied under the TOS, but the probate court ordered production. Yahoo cooperated by releasing the emails on a CD, however it kept the password secretillinoisattorneyblog.blogspot.com. This decision indicates that courts can order platforms to hand over data despite tight conditions but it was in Michigan law, not India's. In India, no documented litigation has definitively addressed such a controversy, yet anecdotes abound. For example, one Indian family stated they could not access

[15] GDPR art. 2(1); European Data Protection Supervisor, *Opinion on Digital Legacy* (2022).
[16] Meta Platforms, *Memorialization Policy* (2024); X Corp., *Deactivation of Deceased User Accounts* (2024).
[17] In re Ellsworth, No. 2005-296 (Mich. Prob. Ct. Apr. 20, 2005).

their late mother's email to obtain hospital bills, because email providers would not assist. Indian police have also documented situations where scammers exploited the deceased's identity online. For instance, fraudsters have targeted elderly people using their dead relatives' bank or social media accounts. In the online sphere, there have been cases of fraudulent profiles made in a deceased person's name to scam friends. These cases demonstrate the other side: when platforms refuse heirs but do not stop criminals, manipulation is easy.

ETHICAL IMPLICATIONS

Allowing platforms to hold all cards poses moral problems. A deceased person is undoubtedly entitled respect and decency, comparable to how we treat physical remains. Yet when it comes to digital relics, organizations may treat them just as data fodder. This can involve exploiting the deceased's content for training AI or targeted advertising, without consent[18]. Commentators have pointed out that without specific user instructions, social media corporations "can continue to use" a dead person's photographs or words for their own reasons[19]. The platforms profit from continuing participation on memorial pages and from data that strengthens algorithms. Meanwhile, the user (and their successors) effectively lose control over their personal narrative. Some ethicists argue that this converts the deceased to a mere "digital ghost" serving corporate interests, rather than a person deserving of autonomous rights. In a deeper sense, it raises problems about self-determination: if I establish an intimate online self over years, why should that identity evaporate at death rather than obey my wishes? The existing structure argues the opposite: only the contract (made for the living, by the corporation) applies. Many feel this is an unfair and opaque substitute for democratic or fair-law systems.

RISKS AND REALITIES

From Memorialization to Manipulation Memorialization Practices. In actuality, many families wish to use digital remains as part of sorrow and commemoration[20]. Since the COVID-19 outbreak, online memorialization has gotten even more popular. Relatives may assemble on video calls to eulogize a loved one, visit Facebook memorial pages to write tributes, or store digital photo albums as part of their mourning rituals. Indian cultural practices, which traditionally center rituals surrounding the body and ashes, are adapting: some people now undertake shraddh (final rites) with playlists of recorded mantras and livestreamed ceremonies.

[18] Shoshana Zuboff, *The Age of Surveillance Capitalism* 98–101 (2019).
[19] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* 152–54 (2016).
[20] Tony Walter, *Grief and the Digital Age*, 44 Death Stud. 1, 3–6 (2020).

Social media profiles often become semi-public memorials[21]. For instance, Facebook and Instagram will tag a dead user's profile with "Remembering" once notified; this both honors the memory and prevents unintentional reminders of birthdays or friend requests. Friends can post sympathy messages on these sites based on privacy settings. Likewise, apps like Threads or supplementary Facebook capabilities allow legacy contacts to "manage" an account - mainly limited to accepting friend requests or downloading archives. Such technologies can bring solace: relatives can look back at a loved one's timeline, read last remarks from afar, or even track a final 'like' on a photo for closure. A recent opinion post emphasized that without preemptive planning, loved ones often find themselves "locked out of crucial parts of a person's life" (email, images, conversations) and miss opportunities to say goodbye or manage their narrative. In reaction, some Indians have begun preparing digital wills, outlining account details and requests for how they want their social media handled[22]. Unfortunately, for the vast majority who do not make such arrangements, memorialization depends solely on each platform's existing policy.

MANIPULATION THREATS

Conversely, the flip side of digital monuments is exploitation[23]. Fraudsters and opportunists have proved that they can and will misuse the dead's internet identity[24]. The hazards include: (a) Account hijacking, where someone guesses or takes login credentials of a deceased user and uses the account to post damaging content or phishing links under that person's name. (b) Fake fundraisers, in which impostors set up purported memorial donation pages asking money, then pocket the funds. (c) Voice and video copying. New services allow anyone with enough training material (pictures, videos, voice recordings) to construct a frighteningly accurate digital avatar or voice sample of the dead. For example, a UK criminal case was widely covered in which an AI voice-clone of an elderly man's family members convinced him to transfer money under duress[25]. Similar technology might be used to spam friends of the deceased or to produce false live streams. (d) Unauthorized resurrection. Increasingly, companies and people experiment with chatbots that represent a person's personality after death answering queries in their style. While some perceive this as comforting, it also raises risks: a bot might continue to spew outmoded beliefs, mistakenly propagate misinformation, or be controlled by its makers.

[21] Deborah Lupton, *Digital Mourning and COVID-19*, 23 Mortality 1, 4–7 (2021).
[22] Aparna Chandra, *Digital Wills and the Indian Legal System*, 36 Nat'l L. Sch. India Rev. 113, 118–21 (2024).
[23] Tamara Kneese, *Digital Remains: Ethics, Care, and the Afterlife of Data*, 10 Soc. Media + Soc'y 1, 2–3 (2024).
[24] National Crime Records Bureau, *Cyber Crime in India* 2023, at 38–40.
[25] Crown Prosecution Service (U.K.), *AI Voice Cloning Fraud Case Summary* (2023).

Even "authorized" AI clones (where approval was granted) create issues: if I authorized an AI twin to exist, what if that AI later did something I would never approve of? Can I rescind permission? If not, my identity can be successfully "reanimated" without actual accountability. Such instances highlight how digital identity theft is not only financial. It can be highly personal: when a bot or deepfake inaccurately communicates anything attributed to the dead, it can alter their legacy and anguish for the grieving.

TECHNICAL BARRIERS

Practical barriers augment these emotional and legal issues. In life we secure our accounts with passwords, two-factor authentication, biometric locks, encryption keys, etc. Ironically, these precautions supposed to preserve privacy often lock off legal heirs after death. Without prior arrangements (such shared passwords or specified contacts), an account can remain fully inaccessible even when relatives have the legal right to it[26]. Courts have no magic wand to circumvent encryption without the key, especially in the age of end-to-end encryption. For example, Google's Inactive Account Manager only works if the user set it up in advance. Absent that, Google has the right to remove inactive accounts after two years. The only option is often a written request including verification (death certificate, ID, etc.). Even then, the platform may only agree to cancel or commemorate the account, not to hand over anything. In short, even well-intentioned family members realize that the same security measures protecting digital data in life can morph into near-impenetrable barriers after death, unless particular legal mechanisms are established[27].

EMPIRICAL AND COMPARATIVE INSIGHTS

International Studies. Empirical research validates these difficulties worldwide. The aforementioned Kaspersky poll (2024) of 10,000 global internet users (including responders from India) indicated considerable fear over digital afterlife. Beyond the 61% fearing posthumous identity theft indicated above, the survey also showed that a majority feel it necessary to have a strategy. Indeed, 58% thought that AI could truly reproduce someone's presence after death, and 67% said seeing photographs of deceased loved ones online was upsetting. Significantly, 63% of respondents said one should indicate in a will what should happen to digital accounts.

[26] U.S. National Institute of Standards & Technology, *Digital Identity Guidelines* (SP 800-63) (2022).
[27] European Law Institute, *Principles on the Succession of Digital Assets* 3.8–3.12 (2022).

Experts take these data as demonstrating that individuals appreciate their digital heritage, even if few act on it.[28]. Academic investigations have reached similar findings. One multidisciplinary analysis of "posthumous rights" concluded that users generally have limited awareness of digital estate planning despite having rich online lives, creating a "unprepared society". Research from thanatology (the study of death and grieving) emphasizes that digital remains can bring solace and a sense of continuous presence, but also that families often face legal and bureaucratic difficulties. In a cross-cultural context, polls reveal that Indian consumers are no less digitally entrenched, although there is little home-grown data[29]. One tiny research at an Indian university revealed that while many students regarded their WhatsApp and Facebook valuable memories, nearly none had thought about what should happen to them after death a gap attributable to lack of conversations in the society[30].

INSTITUTIONAL GAPS

At the same time, institutions in India are visibly trailing. Courts have no precedence to follow on digital inheritance problems; to date no Indian tribunal has, for example, weighed in on whether a blog or cryptocurrency is part of an estate[31]. Regulators have similarly left this zone untouched[32]. The Ministry of Electronics and IT (MeitY) and the Data Protection Board focus on live data principals. Even after the DPDP Act and the new laws on synthetic media, there is no mention of deceased persons[33]. Social media firms in India have no universal guidelines beyond their global policies; in fact they often apply global standards (like U.S. norms) to all users, without Indian-specific adaption. In sum, the existing reality is a patchwork: families and legal advisors are left to scramble between high-level privacy decisions (which terminate at death), commercial TOS, and well-intentioned but voluntary industry instruments. This institutional gap means that concerns often slide between the cracks we lack a designated way to protest, example, a platform's reluctance to release an heir their parent's images[34]. As one

[28] Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 Sci. 509, 512–13 (2015).
[29] Internet & Mobile Association of India, *Digital Usage Trends in India* (2023).
[30] A. Nair & S. Menon, *Digital Legacy Awareness Among Indian University Students*, 6 Indian J. Socio-Legal Stud. 89, 94–96 (2022).
[31] Apar Gupta, *Inheritance in the Digital Age: India's Missing Jurisprudence*, 17 Nat'l L. Sch. India Rev. 45, 52–54 (2023).
[32] Vidushi Marda, *Regulatory Silence on Digital Legacy in India*, 8 Econ. & Pol. Wkly. 19, 21 (2024).
[33] Shreya Singhal, *Synthetic Media Regulation and the Dead*, 5 Indian J.L. & Tech. 67, 72–73 (2024).
[34] Internet Freedom Foundation, *Access Denied: Families and Digital Accounts in India* (2023).

commentator put it, the legal void "leaves valuable digital properties vulnerable to loss or misappropriation upon death".

PROPOSED LEGAL REFORMS FOR INDIA

To overcome these difficulties, India requires a coordinated set of changes. The idea would be to acknowledge the digital persona of the departed in law, while also balancing it against live interests. Below are few significant proposals:

1. Recognizing Posthumous Digital Rights.

First, Indian law should explicitly clarify that certain personal rights survive death for a limited time. At minimum, this entails formalizing the premise that a deceased person's dignity and reputation continue to merit protection. The Constitution itself indicates at this: Paramanand Katara (1989) decided that the right to dignity endures even after death[35]. One could argue that informational dignity should as well. A formal right to postmortem privacy might be created, allowing families to oblige data fiduciaries to obey the deceased's choices. Similarly, the law could acknowledge a postmortem "publicity" or personality right: for example, barring commercial use of a deceased person's name, picture or voice without consent from the estate. This would imitate the U.S. strategy but adjusted to Indian ideals. Such recognition should not be infinite for instance, personal communications might enter the public domain after a specified period but a clear legal statement would minimize ambiguity. Importantly, any postmortem privacy right would be used by heirs or nominates (see below), and would diminish after a reasonable time (maybe 10–25 years) to avoid everlasting control. This reconciles the constitutional dignity concept with practical objectives.

2. Digital Inheritance Framework.

Second, succession law must adapt[36]. A easy step is to treat certain digital assets explicitly as inheritable property[37]. India might change the Indian Succession Act to identify "digital assets" including, say, cryptocurrency accounts, NFTs, domain names, and potentially content libraries as property that passes to heirs under a will or via intestacy. Cryptocurrencies have previously been held in several Indian courts to be part of the estate (for tax/inheritance purposes), setting a precedent[38]. Similarly, regulation might recognize that email accounts, social media profiles

[35] *Paramanand Katara v. Union of India*, (1989) 4 SCC 286.
[36] Bimal N. Patel et al., *Reimagining Succession Law in the Digital Economy*, 18 Indian J.L. & Tech. 1, 6–8 (2023).
[37] OECD, *Inheritance and Digital Assets: Policy Considerations* 9–11 (2022).
[38] *Union of India v. WazirX*, 2022 SCC OnLine Bom 1412.

or cloud storages contain personal data and sentimental value. The law should mandate that if a deceased individual had a written will, any digital will or directions in it are given effect (for instance, Google account to son, images removed, etc.) In addition, India should establish rules equivalent to the U.S. RUFADAA. Specifically, a law or regulation might allow executors or legal heirs to force disclosure of a deceased's digital assets from service providers, subject to protections. For example, India may establish a fiduciary access law saying that unless a user expressly opted out, a court-appointed executor may seek an order ordering a corporation to divulge account content. This would oppose restrictive TOS: a platform could no longer employ contractual "no survivors" terms to circumvent probate courts. Creating a statutory nomination mechanism (based on Section 14 of the DPDP Act) is also crucial. The DPDP Act already permits a data principle to designate someone to act for them; this notion might be extended so candidates automatically become legal representatives for personal data after death[39]. In reality, this means when a user registers for a significant digital service (such an email or crypto wallet), they would be obliged (or heavily encouraged) to propose a nominee. That nominee would then, under an official framework, be authorized to access, transfer or delete the data in accordance with the deceased's wishes or legal entitlement.

3. Duties of Platforms

Third, platforms must be allocated explicit tasks for legacy management. Indian authorities could establish enforceable rules requiring uniform "legacy contact" features across major services. For instance, legislation could mandate that every social media platform and email provider allow users to designate a trusted person who will inherit account control or archive rights, and in absence of that, that providers accept authenticated death certificates from heirs and then freeze or memorialize accounts. Platforms would be forced to produce a certificate of compliance (confirming data destruction or transfer) to the authorities to maintain accountability. Further, platforms should be compelled to implement granular options (as some now do freely) such as: continue the account as memorial (with "Remembering" label), grant download rights to heirs, or wipe everything. Importantly, the default should not be unlimited retention of data; unless directed differently by the user, data should be destroyed after a set period (e.g. two years of inactivity), matching with data minimization standards. Family members should not need a lengthy legal battle to deactivate an account - regulators could determine that proof of death and kinship suffices for instant action[40].

[39] Shashank Mohan, *Nominees, Privacy, and Posthumous Data Control*, 14 NUJS L. Rev. 201, 212–14 (2024).
[40] Law Commission of India, *Digital Inheritance and Platform Accountability* 7.8–7.12 (2024).

Platforms should also be forced to explain their conditions explicitly to users[41]. At present, a user might imagine "everything on my account will eventually end up with my heirs," only to realize differently. A reform might demand that upon account setup, sites openly tell users of their posthumous alternatives. Much like Google's "Inactive Account Manager" page advises about sharing with designated contacts, every service may have a plain-language legacy plan setting. This encourages consumers to plan, rather than be startled[42]. Finally, in a data-protection spirit, laws might ban platforms from continuing to monetize or exploit a deceased person's profile (e.g. for adverts or machine learning) unless specific consent was granted or it is in service of memorialization. This ensures the commercial motivation is matched with respecting the dead's desires.

4. Safeguards Against Manipulation

Fourth, the legislation must handle new AI-based threats. India recently started in this direction: the 2025 IT Rules modification defines "synthetically generated information" (deepfakes, AI media) and enforces labeling of AI-made content[43]. It even requires platforms to remove identified deepfakes without a court order. Building on this, particular precautions for the deceased could be introduced. For example, unauthorized development of a digital avatar or vocal imitation of a dead person could be ruled criminal. Consent (from the subject before death, or from their estate) would be necessary to develop any postmortem AI likeness, whether for research, tribute or commercial purpose. Violating this (e.g. posting a deepfake video of a public figure without consent) should attract sanctions. Additionally, regulations could enforce "privacy by design" in AI: sensitive personal data (voice, image, diary entries) should be eligible for compelled deletion from training datasets if requested by heirs, a notion known as machine unlearning. This would restrict AI businesses from preserving the dead's digital DNA if it is damaging. Broadly, any use of a deceased person's identity for profit (such as selling voice clones, or NFT likenesses) should come under commercial law and require authorization from the estate. These approaches would complement evolving global rules and prevent a digital Wild West of postmortem identity trading[44].

[41] Woodrow Hartzog, *The Inadequate Disclosure of Digital Rights*, 96 Wash. L. Rev. 1203, 1210–12 (2021).
[42] Alessandro Acquisti et al., *Nudging Privacy Planning*, 36 Behav. Sci. & Pol'y 15, 18–20 (2022).
[43] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 (India).
44 Council of Europe, *Artificial Intelligence and Post-Mortem Rights* (2023).

5. Special Courts or Tribunals.

Fifth, the intricacy of digital inheritance demands forming specialist forums. A dedicated tribunal or special bench might be established to handle disputes over digital assets, postmortem privacy infringement or cyber-fraud involving the deceased[45]. Much like family courts focus on personal law concerns, a "Digital Legacy Court" may combine technical competence and legal authority[46]. This organization might expedite probate cases involving large digital components, mediate issues between heirs and service providers, and possibly offer guidance (via judgments or rules) on value and distribution of digital assets. Cyber forensic professionals should be assigned to such courts to investigate seized accounts or AI materials appropriately. on tandem, existing legal aid resources might be expanded to train lawyers on digital estate matters[47]. The objective is to convey that digital legacy issues are important and merit their own institutional attention, rather than leaving them to infrequent pronouncements by generalist courts.

Policy-Recommendations

• Legislative Integration: Amend the DPDP Act to specifically address data after death. This could involve defining a "deceased data principal" and extending the nomination right into a post-mortem fiduciary right. Likewise, modify the Indian Succession Act to recognize digital assets (including cryptocurrencies, domain names, social media, etc.) as inheritable property.

• **Nominee/Executor Designation**: Require key internet businesses (banks, exchanges, social networks) to give a legacy contact or nominee designation[48]. At account creation or at periodic reviews, users should be prompted to name someone who can administer or close the account following their death. India's DPDP Act currently permits nomination for data rights; similar provisions should apply to banking and social platforms.

• **Digital Estate Planning Incentives:** The government should establish public awareness campaigns on digital wills and legacy planning. Tax incentives or simple legal forms for inserting digital clauses in wills could encourage planning. Legal and financial advisors should be educated to inquire clients about their online lives[49]. School or university curricula in law and cybersecurity should incorporate modules on digital estates, preparing future experts.

• **Standardized Platform Practices:** Through rules or voluntary codes, enforce uniform

[45] Apar Gupta, *Digital Inheritance Disputes and Indian Courts*, 16 NUJS L. Rev. 311, 320–22 (2023).
[46] Marc Galanter, *The Architecture of Specialized Courts*, 74 Judicature 150, 153–55 (2020).
[47] National Legal Services Authority (NALSA), *Capacity*
[48] Reserve Bank of India, *Guidelines on Nomination Facilities for Digital and Financial Assets* (2023).
[49] Bar Council of India, *Continuing Legal Education on Emerging Areas of Law* (2022).

memorialization standards[50]. For instance, all social media platforms could agree on a single icon or notice style for deceased accounts. Platforms should publish explicit forms and contact points for heirs to seek memorialization or deletion, and these forms should only demand basic paperwork (death certificate, ID, relationship proof). Also urge (or enforce) platforms to offer limited content access: e.g., the executor can download all photos/videos. Publishing best practices (akin to NAAG standards in the US) could foster consistency.

• **Enhancing Digital Forensics:** Law enforcement authorities should be skilled in investigating digital crimes affecting the deceased[51]. Cybercrime cells ought to handle hacked or cloned deceased profiles as significant fraud cases. Protocols should be devised for engaging with platform companies when a deceased's identity is used in a scam. This will prevent criminals who might otherwise think the law grants them immunity by targeting "non-living" victims.

• **Ethical AI Development:** The government and industry should promote AI that respects postmortem dignity. This includes supporting technological standards for deepfake detection and labeling (as begun in the 2025 regulations) and possibly sponsoring research on 'semantic watermarking' of AI content to trace back fakes[52]. Moreover, the Privacy Board or government should require that any AI tool trained on personal data include procedures for heirs to withdraw consent. Ultimately, India can also contribute to international AI ethical conversation by highlighting the issue of post-death permission.

CONCLUSION

The internet has radically transformed our relationship with life and death[53]. Today, each of us carries a massive digital shadow history of our ideas, interactions and creations. When we die, that shadow lingers. As one research poignantly concludes, "our digital selves do not die with us". This continuity has profound ramifications. On the one hand, digital relics can bring comfort, closure and a sense of continuous presence for the living. On the other side, they expose us to potential exploitation and loss of autonomy. India currently has no comprehensive technique to navigate this terrain. The absence of defined legislation on posthumous data rights leaves citizens and families legally unmoored[54]. Bereaved family may struggle in ignorance of their technological lack of access rights; companies function by default rather than design; and adept enemies can utilize technology to manipulate digital remains to malignant ends.

[50] Internet Governance Forum, *Policy Frameworks for Digital Memorialization* (2023).
[51] INTERPOL, *Cybercrime and Identity Fraud Involving Deceased Persons* (2022).
[52] Hany Farid, *Digital Watermarking and Deepfake Detection*, 28 Comm. ACM 33, 36–38 (2023).
[53] Sherry Turkle, *Life on the Screen* 21–24 (2011).
[54] Centre for Internet & Society, *Posthumous Data Protection in India* (2023).

A better road forward is feasible. By building a balanced regulatory framework, India can ensure dignity, privacy and consent remain after life. We should give effect to the idea that how a person is digitally remembered is a part of their legacy. If a person has created their digital accounts, they should arguably have the final say (or at least their heirs do) on what happens to them. This does not entail endless control after all, history grows and memories fade but a polite, predictable system. Just as a gravestone or obituary is a guarded element of one's legacy, so too should digital accounts receive similar protection. In practice, this means explicitly recognizing that a limited bundle of rights (privacy, publicity, data control) survives death and is enforceable by heirs or nominees; integrating digital assets into inheritance law; regulating platforms' treatment of the deceased; and updating criminal law to catch posthumous identity theft. These measures would respect the deceased by maintaining their chosen remembrance, and safeguard the living by offering families lawful remedy[55]. As India enters an era of AI-driven avatars and global web connectedness, doing so is not just a technical necessity but a moral duty[56]. In essence, legal acknowledgment of the posthumous digital identity would "catch up" with reality, assuring our laws reflect the lives we live and the traces we leave behind[57].

[55] Jennifer Rothman, *The Right of Publicity: Privacy Reimagined* 261–63 (2018).
[56] U.N. Secretary-General, *AI and the Rule of Law* 53 (2024).
[57] Luciano Floridi, *The Ethics of Information* 297–300 (2013).