



# The Unfinished Digital Estate

## Culture, Law, and Technology after Death

3 March 2026

Editors:

Heather Flanagan

Mike Kiser

Dean H. Saxe

# Contributors



In addition, this paper would not have been possible without the support of several individuals who generously offered their time and knowledge to inform the content and themes presented here.

- George Fletcher (Practical Identity LLC)
- Sasikumar Ganesan (MOSIP)
- Eve Maler (Venn Factory)
- Ramesh Narayanan (MOSIP)
- John Scullen (Australian Access Federation)  
ORCID <https://orcid.org/0000-0002-0390-4377>
- Jennifer Zegel (Kleinbard LLC)
- OI DF's Death and the Digital Estate Community Group members

Citation:

Flanagan, Heather, Mike Kiser, and Dean H. Saxe, eds. "The Unfinished Digital Estate: Culture, Law, and Technology After Death." OpenID Foundation, March 3, 2026. <https://openid.net/wp-content/uploads/2026/03/The-Unfinished-Digital-Estate-Final.pdf>

Date	Revision
21 August 2025	Public Draft released
3 March 2026	Publication of final v 1.0

## Editors' Note on Use of AI Tools

This paper is the result of research and drafting conducted by the authors. The core arguments, analysis, and writing were developed by people. ChatGPT was used as a tool to assist with polishing language, harmonizing tone, and formatting references. All substantive ideas and conclusions remain the work of the authors.

## Table of Contents

<b>Executive Summary</b> .....	<b>5</b>
<b>1 Death in the Digital Age</b> .....	<b>6</b>
<b>2 Cultural Perspectives on Death and Their Impact on Digital Estate Planning</b> .....	<b>7</b>
2.1 <i>Cultural Variations in Death Practices</i> .....	8
2.1.1 Western Cultures.....	8
2.1.2 Eastern Cultures .....	9
2.1.3 African Cultures .....	10
2.1.4 Indigenous Cultures .....	11
2.2 <i>Implications for and Influence on Digital Estate Planning</i> .....	12
2.2.1 Perception of Digital Assets .....	12
2.2.2 Communication Styles and the Planning Gap .....	12
2.2.3 Family Dynamics and Decision-Making Models.....	13
2.2.4 Customization of Planning Tools.....	13
2.2.5 Education and Awareness .....	13
2.2.6 Policy Development.....	14
<b>3 Who and What Is at Risk</b> .....	<b>14</b>
3.1 <i>Emotional Cost</i> .....	14
3.2 <i>Financial Risk</i> .....	15
3.3 <i>Abuse, Exploitation, and Fraud</i> .....	15
3.4 <i>Loss of Identity Autonomy</i> .....	16
3.5 <i>Special Populations at Heightened Risk</i> .....	16
3.6 <i>Public Awareness is Low</i> .....	16
<b>4 Legal and Regulatory Touchpoints</b> .....	<b>17</b>
4.1 <i>A Patchwork of Protections</i> .....	17
4.2 <i>Jurisdictional Silos and Systemic Gaps</i> .....	18
4.3 <i>International Signals, but Global Incoherence</i> .....	18
4.4 <i>Global Landscape: Digital Estate Planning by Region</i> .....	18
4.4.1 United Kingdom .....	19
4.4.2 Japan.....	19
4.4.3 Australia .....	19
4.4.4 India .....	19
4.4.5 European Union .....	19
4.4.6 South Africa: Legal Foundations and Emerging Practices.....	19
4.4.7 Nigeria: Navigating Legal Ambiguities.....	20
4.4.8 Tanzania: Calls for Legal Frameworks .....	20
4.4.9 Other Regional Initiatives in Africa: Pollicy's "Mine is Yours" Project.....	20
4.5 <i>Industry Approaches to Digital Asset Estate Planning</i> .....	21
4.5.1 Financial Services.....	21
4.5.2 Technology Sector.....	21
4.5.3 Healthcare Industry.....	21
<b>5 The Technology Landscape</b> .....	<b>22</b>

5.1	<i>Fragmented Tooling and Uneven Coverage</i> .....	22
5.2	<i>Where Technical Models Do Exist</i> .....	23
5.3	<i>The Interoperability Gap</i> .....	25
5.4	<i>A Path Forward</i> .....	26
<b>6</b>	<b>Delegation, Guardianship, and Identity Transitions</b> .....	<b>27</b>
6.1	<i>Delegation Semantics: Impersonation vs. Acting on Behalf Of</i> .....	28
6.2	<i>Technical Basis: Tokens and Transitions</i> .....	28
6.3	<i>Evolving Models for Guardianship and Shared Authority</i> .....	29
6.4	<i>Cultural Norms in Law and Family Authority</i> .....	29
6.5	<i>Delegation Threat Models and Abuse Scenarios</i> .....	30
6.5.1	<i>Elder Abuse and Financial Exploitation</i> .....	30
6.5.2	<i>Partner and Domestic Abuse</i> .....	30
6.5.3	<i>Institutional Overreach</i> .....	31
6.5.4	<i>Inheritance Without Intent</i> .....	31
<b>7</b>	<b>Posthumous AI and the Question of Digital Humanity</b> .....	<b>31</b>
7.1	<i>Persistence Through Synthetic Media</i> .....	31
7.2	<i>Consent and Control</i> .....	32
7.3	<i>Legal and Ethical Questions</i> .....	33
<b>8</b>	<b>Policy and Standards Recommendations</b> .....	<b>34</b>
8.1	<i>Policy Priorities for Legislators and Regulators</i> .....	34
8.2	<i>Recommendations for Standards Bodies</i> .....	35
8.3	<i>Implementation Pathways and Cross-Sector Collaboration</i> .....	36
<b>9</b>	<b>Conclusion</b> .....	<b>37</b>
<b>10</b>	<b>Appendices</b> .....	<b>39</b>
10.1	<i>Bibliography</i> .....	39

# Executive Summary

Digital life now extends beyond our lifespans, but most societies remain unprepared for what happens when people die or become incapacitated while leaving behind significant online assets. Bank accounts and crypto wallets are only part of the story. Email, shared photos, creative work, credentials, playlists, social media profiles, and connected devices all form a digital estate that outlives its owner.

The problem is both cultural and structural. Around the world, traditions shape how families grieve, honor, and make decisions about the deceased. Digital estates complicate those traditions, blurring the lines between property, privacy, and personhood. Legally, inheritance systems rarely account for digital assets. Most platforms treat death as an edge case. The handful that have implemented features still leave executors and relatives to navigate fragmented tools and opaque policies.

We face a growing set of challenges in managing digital assets. Families face emotional distress or cannot successfully manage when locked out of accounts or confronted with unwanted algorithmic reminders. Valuable assets, such as cryptocurrency, monetized content, and cloud files, can vanish or fall prey to fraud. Exploitation risks rise through impersonation, deepfakes, or coerced access. Without safeguards, a person's digital identity may be altered or erased against their wishes.

As it stands now, global approaches are uneven and inconsistent. The United States' Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) model provides partial access rights but defaults to platform terms of service (Fiduciary Access to Digital Assets Act, Revised). Japan urges citizens to document account credentials, but adoption remains low. Europe is exploring harmonized rules, while African initiatives like Pollicy's "Mine is Yours" project aim to raise awareness. Industry responses are patchy: some tech firms offer legacy tools, but approaches and coverage are inconsistent and inadequate.

Some early models in this space show promise. Sovrin's guardianship credentials and Kantara's User-Managed Access (UMA) framework demonstrate how verifiable, revocable, and auditable delegation could work. Legal scholars highlight the complexity of minors' data, shared accounts, and cross-jurisdictional conflicts.<sup>1</sup> The Modular Open Source Identity Platform's (MOSIP's) work on integrating death registration illustrates both progress and limits, underscoring the absence of a full "digital estate lifecycle."

AI introduces further complications. Posthumous avatars and synthetic media force society to confront whether digital humanity should persist, and on what terms. Recent cases highlight the risks of unauthorized recreations, deepfakes, and contested rights of publicity.

Policymakers must formally recognize digital assets, extend estate law, and protect and clarify identity rights after death. Standards bodies must design interoperable delegation protocols, verifiable triggers for incapacity or death, and trust frameworks for estate

---

<sup>1</sup> Kantara Initiative, "User-Managed Access"

services. Platforms must move beyond credential sharing and impersonation to on-behalf-of delegation with clear consent, revocation, and auditability. Civil society must raise awareness, provide planning tools, and advocate for inclusive approaches that respect cultural diversity.

Digital estate planning is no longer a niche concern. Protecting privacy, preventing abuse, and preserving what matters requires governments, industry, and communities to act together. Without coordinated standards and policies, digital legacies remain vulnerable, and the living bear the consequences.

## 1 Death in the Digital Age

As more and more people are born into the digital age, we are also entering a time where more and more people die or become incapacitated while leaving behind significant digital assets. These aren't just bank accounts and crypto wallets. They are the email accounts, shared photos, online identities, finished and unfinished creative work/intellectual property, credentials, playlists, social media profiles, and smart devices that are still quietly running in the background.

This is becoming our new normal. And yet, as a global society, we have failed to address the inevitable.

Most legal systems lack clear guidance on the transfer of digital rights. Most technology platforms still treat death as an edge case, if they acknowledge it at all. And most people haven't made decisions about how their online presence should be handled when they're gone, because we haven't been taught how to think about it.

Part of the problem is cultural. Around the world, death is handled in very different ways, from private, pragmatic planning to communal rituals that extend for generations. But digital life complicates all of that. Where traditional inheritance laws handled the transfer of tangible assets, digital estates blur the line between property, privacy, and personhood. Can your email be inherited? Should your AI avatar be switched off, or should it be improved?

And part of the problem is structural. Current estate tools are designed for paper trails and legal heirs, rather than for shared passwords, joint cloud folders, or semi-public social media personas. Some users rely on platform-specific tools, such as Facebook's Legacy Contact or Google's Inactive Account Manager. Others just hope that a trusted friend knows the right login information. But there's no common protocol, no industry standard, and no guarantee that a deceased person's wishes—or their family's needs—will be honored.

In this paper, we explore what happens when digital identity outlives the person it belongs to, and what we can do about it. We'll look at the legal frameworks (like the Revised

Uniform Fiduciary Access to Digital Assets Act (RUFADAA)<sup>2</sup> and postmortem publicity rights), the technical models (like Kantara’s User-Managed Access (UMA)<sup>3</sup> and guardianship credentials), and the cultural influences that shape how we grieve, remember, and manage what remains.

If we want to protect privacy, prevent abuse, and preserve what matters, we need to treat digital estate planning not as a niche concern but as a shared societal responsibility.

## 2 Cultural Perspectives on Death and Their Impact on Digital Estate Planning

While death is a universal part of human experience, cultures around the world vary widely in how they interact with both the deceased and the bereaved. The values and beliefs of each cultural system are reflected in ceremonies, rituals, and perspectives<sup>3</sup> that enable the community to mark and process the event.

As we build digital landscapes that acknowledge and cater to the full human lifecycle, it is important that we understand the entire cultural infrastructure: what each culture values, what principles they represent, and how those translate into concrete legal or societal processes to allow for the assimilation of the death of a community member. As Mandebaum wrote in “Social Uses of Funeral Rites”:

*“. . . certain things must be done. The corpse must be disposed of, those who are bereaved — who are personally shocked and socially disoriented — must be helped to reorient themselves; the whole group must have a way of readjustment after the loss of one of its members (Feifel 1959, 189).”<sup>4</sup>*

Without this understanding, we risk reinforcing the cultural lens of a specific perspective rather than supporting the entire spectrum of beliefs and practices.

What follows is not an exhaustive list of cultural practices, but rather snapshots of current societal systems. These are intended to allow the reader to imagine what cultural values are driving the practices in whatever society they may find themselves in, as well as to broaden their view of how humanity responds to the reality of death through ceremony and (digital) estate planning.

---

<sup>2</sup> “Fiduciary Access to Digital Assets Act, Revised,” Uniform Law Commission, 2015, accessed December 17, 2025, <https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22>.

<sup>3</sup> Kantara Initiative, “User-Managed Access: Taking Control of Your Data Sharing | Kantara Initiative,” May 9, 2025, <https://kantarainitiative.org/work-groups/uma/>.

<sup>4</sup> Herman Feifel, *The Meaning of Death* (McGraw-Hill Companies, 1959).

## 2.1 Cultural Variations in Death Practices

In *The Broken Connection*, Robert Jay Lifton proposed a framework to describe the basis by which a culture approaches death and seeks to promote what he called “symbolic immortality,” thereby providing continuity for the society (Lifton, 1996).<sup>5</sup> It is helpful to consider these components when examining a cultural viewpoint or practice.

Lifton’s framework describes “symbolic immortality” in five modes: biological, theological, creative, via nature, and experiential transcendence. Continuity is provided in different forms to allow a society to “confront genuinely the fact that we die (Palgi and Abramovitch 1984, 392).”<sup>6</sup> (1) Biological continuity comes via not only genetic connections to family, but also strong, continuous connections to groups that we belong to: tribe, people, nation, etc. (2) Theological continuity is provided through a belief system in an afterlife or equivalent that allows for a space where “one is offered the opportunity to be reborn into a timeless realm of ultimate death-transcending truths.” (3) Creative continuity is established through the act of creation—influences or works that will live on past the individual. (4) Nature provides continuity through its relative permanence; mountains, rivers, and oceans all will last beyond the current timeframe. The final potential mode is (5) experiential transcendence. This is a mystical state that provides continuity through an experience rather than any cognitive belief.

### 2.1.1 Western Cultures

Western cultures have gone through a progression of approaches to death over the centuries, with the most recent cultural approach reinforcing the trend to avoid death and discussions of death if possible. Death is, in effect, a taboo subject for many of these cultures, particularly as they become increasingly secular.

In part, this is seen in how society handles death. The tendency is to isolate the dying, even from any potential “biological” or familial continuity; they are removed to a hospital where the medical system takes over, providing anonymity and taking them out of the cultural context of their families and communities. It is not merely the dying person who tends to be isolated, either; survivors are also isolated from contact with their loved ones. French historian Philippe Ariès sees this as if the society views death as a “massive admission of defeat,” writing, “We ignore the existence of a scandal that we have been unable to prevent. We act as if it did not exist . . . (Palgi and Abramovitch 1984, 408).”<sup>7</sup> (It is worth noting, of course, that the rise in hospice care belies a counter movement against this, with a small subset of the culture seeking to recover human dignity in the face of death.)

---

<sup>5</sup> Robert Jay Lifton, *The Broken Connection: On Death and the Continuity of Life* (American Psychiatric Pub, 1996).

<sup>6</sup> Phyllis Palgi and Henry Abramovitch, “Death: A Cross-Cultural Perspective,” *Annual Review of Anthropology* 13, no. 1 (October 1, 1984): 385–417, <https://doi.org/10.1146/annurev.an.13.100184.002125>.

<sup>7</sup> Ibid.

This expediency does not end with the medical process, either. Western cultures tend to have a relatively rapid process for the registration of death and the (often) quick funeral ritual that follows. This may lead to a lack of processing by the survivors, and may also intensify the desire not to speak of death outside of these narrow windows.

This taboo status obviously has implications for how these cultures approach estate planning and the management of digital estates. Conversations about “what happens when someone dies” are often avoided, leaving the approach to be undiscussed and unplanned. This is particularly true of digital lives, which are a more recent development even in Western cultures.

### 2.1.2 Eastern Cultures

Eastern cultures tend to view death differently. Rather than a topic that is avoided, death is seen as a rite of passage, a natural next phase of a cycle. Two of the predominant religions of the East (Hinduism and Buddhism) incorporate the concept of reincarnation into their worldview, which contemplates death as the entry into the next phase, whatever that may be.

Rituals often mark various phases in life, from prebirth to childhood to educational milestones to marriage to death. In Japan, for instance, there are markers for at least ten auspicious birthdays: sixtieth, seventieth, seventy-seventh, all the way up to one-hundred-eleventh) (Yohko 2011, 30).<sup>8</sup> These provide markers that serve as culturally guarded rites of passage leading to death.

And when combined with close familial and collective ties, this impacts the concept of death significantly. As Rao writes in reference to a specifically Hindu approach to counseling the dying,

*“It is the dharma of the individual to act correctly and perform their roles in the context of her/his society and family, and therefore the ‘autonomous individual’ of the modern West is not the kind of person that you would find in the Hindu context. Family is important, and end of life care decisions are made in consultation with or by the family, depending on the circumstances of the particular individual (Rao, n.d., 71-72).”<sup>9</sup>*

Other cultures in the East also adopt practices that incorporate the deceased into everyday life. In China, ancestor worship has been “one of the central institutions of Chinese society

---

<sup>8</sup> Yohko Tsuji, “Rites of Passage to Death and Afterlife in Japan,” *Journal of the American Society on Aging* 35, no. 3 (2011): 28–33, <https://www.jstor.org/stable/26555791>.

<sup>9</sup> Ramesh N. Rao, “TALKING TO THE DYING: Hindu Views, Hindu Ways,” *International Journal of Sociology of the Family* 36, no. 1 (2010): 65–76, <https://www.jstor.org/stable/23070779>.

regardless of temporal and geographic boundaries (Clarke 2000, 273).<sup>10</sup> Japan likewise honors past family members who have died, including regular visits to the family grave, and celebrations for ten death anniversary rituals up to fifty years postmortem.

These family ties and rituals help support and comfort elders because by participating in these rituals, they are reminded that death will not cause them to be forgotten; they will instead be remembered for many years by their families. In fact, since death and the afterlife have a prominent cultural place, many homes for the “elderly also have a common room with a Buddhist altar to remind residents to remember their departed relatives (Yohko 2011, 31).”<sup>11</sup>

These views of death as a passage to the next state, close ties to family and community, and the incorporation of the deceased into everyday life can provide a solid foundation where conversations about estate planning and management of digital life can take place more easily than other cultural contexts.

### 2.1.3 African Cultures

African cultures have a wide set of approaches that cut across the spectrum of responses to death.

Madagascar’s practice of famadihana, in which ancestors are taken out of tombs and wrapped in new silk shrouds, underscores the deep relationship between the living and the dead in that culture. One such story from Graeber’s work on the practice describes how the ancestors might appear in the dreams of the living, requesting a famadihana because they were cold (Graeber 1995, 258).<sup>12</sup> Respecting the wishes of the ancestors ensured blessings for the community, failure to do so came with consequences. It should be pointed out that this practice likely developed as a response to the community previously being enslaved and therefore not able to possess land for burial practices.

Other cultures within the region do not possess the same relationship with the dead. One notable example is “immediate-return societies” such as !Kung and the Pygmies of Central Africa. These societies are “present-oriented, non-accumulating, highly cooperative, pragmatic” (Palgi and Abramovitch 1984, 391).<sup>13</sup> This means that their treatment of the deceased was rudimentary, and there was no indication that an afterlife was a thought for the community. Instead, societies such as these focus on immediate, temporary personal and shared grief.

---

<sup>10</sup> Ian Clarke, “Ancestor Worship and Identity: Ritual, Interpretation, and Social Normalization in the Malaysian Chinese Community,” *Journal of Social Issues in Southeast Asia* 15, no. 2 (October 2000): 273–95, <https://www.jstor.org/stable/41057042>.

<sup>11</sup> Yohko Tsuji, “Rites of Passage to Death and Afterlife in Japan.”

<sup>12</sup> David Graeber, “Dancing with Corpses Reconsidered: An Interpretation of ‘famadihana’ (In Arivonimamo, Madagascar),” *American Ethnologist* 22, no. 2 (May 1995): 258–78, <https://www.jstor.org/stable/646702>.

<sup>13</sup> Palgi and Abramovitch, “Death: A Cross-Cultural Perspective.”

The details of these two examples have clear implications for how they would approach estate planning. In Madagascar, it is essential for the community to honor the dead, to obey their wishes (even after death), and thus, planning for death is a prescribed ritual in itself. By honoring these rituals, the members of the society also help ensure that they will be honored in the same way. In immediate-return societies, estate planning lacks a strong cultural connection for obvious reasons.

#### 2.1.4 Indigenous Cultures

Indigenous cultures vary widely in their views on death and estate planning as well. While the spectrum is fairly wide, a few samples will help to draw out the issues these communities face.

The Kota people of the Nilgiri Mountains in South India have a two-ceremony ritual that seeks to repair and retain social structure while ensuring proper honor and treatment of the deceased. The “Green Funeral” takes place immediately after the cremation of the body, and the “Dry Funeral” occurs once a year and includes all deaths since the last “Dry Funeral.” The deceased is not purified enough to depart for the afterworld until the second funeral is completed, ensuring the proper respect and honor has been paid. Additionally, there is a rigid structure rank maintained for all processions and proceedings. This reminds the community that despite the loss, the social order is maintained and continues (Palgi and Abramovitch 1984, 394).<sup>14</sup>

Other indigenous cultures respond differently, however, including the Hopi and Apache in North America.

The Hopi funeral ceremony is very subdued; the main point is to send off the spirit to a different realm so that the Hopi will not be disturbed in this world. Parsons writes, “No Pueblo Indian of the older generation wants a picture of a deceased relative (Palgi and Abramovitch 1984, 395).”<sup>15</sup>

The Apache paint a more complicated cultural picture, and one that has a direct impact on how the culture accounts for the deceased. The Apache placed opposing demands on its members. On the one hand, family solidarity was required, complete with the avenging of any wrongs inflicted on them. At the same time, the culture valued independent and self-reliant behavior. These conflicting demands meant that there was often resentment due to the demands of close relatives (demands which were often met). This resentment was incorporated into the ritualistic response to death. Couple that with a latent cultural ideal that anyone who gained “supernatural” power (not an uncommon occurrence) was required to suffer the loss of a close relative, and things get a bit complicated. To deal with these cultural demands, an individual was given the chance to mourn loudly and publicly, but after the burial occurred, the community would fully support him in forgetting the loss.

---

<sup>14</sup> Palgi and Abramovitch, “Death: A Cross-Cultural Perspective.”

<sup>15</sup> Ibid.

In short, the obligations to the deceased were complete (Palgi and Abramovitch 1984, 396).<sup>16</sup>

These wide-ranging cultural values and resulting ritualistic responses to death show the challenges and opportunities for estate planning (and *digital* estate planning, depending on where these indigenous people fall on the technological adoption spectrum). Those cultures that want to avoid obligations to the deceased are obviously less likely to be motivated to think through contingencies and plan for their future state. On the other hand, cultures that seek to maintain social order and connections through their rituals would be more amenable to well-defined estate planning.

## 2.2 Implications for and Influence on Digital Estate Planning

Digital estate planning is often framed as a technical or legal challenge. But it is also deeply cultural. How individuals approach the end of life—what they choose to preserve, share, or erase—varies widely across societies. As platforms and policymakers attempt to develop more robust tools for managing digital legacies, they must take into account these differences in values, communication styles, and family dynamics.

### 2.2.1 Perception of Digital Assets

In many cultures, digital assets are not simply property; they are viewed as extensions of the self. In societies with strong ancestral traditions, such as parts of East Asia, sub-Saharan Africa, and Latin America, memorialization is an active, ongoing practice. A digital photo album, blog archive, or social media account may be seen not as data to be deleted, but as a vital link to the past. Preserving these digital artifacts can carry significant spiritual, emotional, and social value, especially when the deceased played an important role in the community.

This contrasts with the legal and technical frameworks in the West, which tend to treat digital assets as disposable or monetizable, often overlooking their relational or ceremonial value.

### 2.2.2 Communication Styles and the Planning Gap

Cultural differences in communication can also affect digital estate planning. High-context cultures, which rely on shared understanding and implicit norms, may not emphasize direct instruction for digital legacy. In these environments, family members may assume responsibility without formal delegation, expecting their actions to align with communal values (Country Navigator, 2023; Techtello, 2023).<sup>17</sup>

---

<sup>16</sup> Palgi and Abramovitch, “Death: A Cross-Cultural Perspective.”

<sup>17</sup> Transnational Management Associates Limited (trading as TMA World and Country Navigator), “Country Navigator | the No.1 Cultural Intelligence Training Platform,” May 20, 2024,

By contrast, low-context cultures prioritize explicit directives. Users are more likely to leave written instructions, designate legacy contacts, or codify digital asset wishes in a will. Planning tools designed only for explicit input may be inaccessible or underutilized in high-context communities, inadvertently excluding users who rely on oral tradition, communal decision-making, or assumed roles.

### 2.2.3 Family Dynamics and Decision-Making Models

In collectivist societies, digital estate decisions are often made jointly or passed to extended kin groups. A sibling, parent, or in-law may manage an account not based on legal designation, but on customary or familial roles (Verywell Mind, 2023).<sup>18</sup> This contrasts with individualistic societies, where autonomy is emphasized and authority is granted through legal instruments, such as powers of attorney or digital asset clauses in a will (Verywell Mind, 2023).<sup>19</sup>

Designing estate planning systems that default to a single, legally designated decision-maker may not accurately reflect how responsibility is actually distributed in practice. Tools that accommodate shared access, co-signing, or role inheritance can offer better alignment with lived family dynamics across diverse cultural contexts.

### 2.2.4 Customization of Planning Tools

Digital estate planning solutions must be flexible enough to support a variety of cultural expectations and legal environments. This may include:

- Multiple delegate types (e.g., ceremonial steward vs. financial executor vs. trustee)
- Language localization and culturally specific defaults
- Options for ritualized content deletion or online memorialization, shared mourning spaces, or preservation of ancestral records

Such features recognize that digital identity is not only individual, but social and intergenerational (ACTEC, 2022).<sup>20</sup>

### 2.2.5 Education and Awareness

In many regions, digital legacy planning is an unfamiliar concept. Without accessible education, users may not realize the risks of inaction or the options available to them.

---

<https://www.countrynavigator.com/> and TechTello, "Learn and Be Better Everyday - TechTello," September 3, 2024, <https://www.techtello.com/>.

<sup>18</sup> Kendra Cherry MEd, "Understanding Collectivist Cultures," Verywell Mind, October 17, 2025, <https://www.verywellmind.com/what-are-collectivistic-cultures-2794962>.

<sup>19</sup> Ibid.

<sup>20</sup> The American College of Trust and Estate Counsel, "The Importance of Cultural Competence in Estate Planning," October 4, 2023, <https://www.actec.org/resource-center/video/the-importance-of-cultural-competence-in-estate-planning/>.

Outreach efforts must consider literacy levels, language access, and cultural norms around discussing death.

For example, public health campaigns in Japan have encouraged people to include passwords in estate planning. In other countries, civil society groups have begun offering “digital legacy workshops” in community centers or faith institutions. Broadening these efforts can help normalize planning and reduce confusion during moments of loss (STEP, 2022).<sup>21</sup>

## 2.2.6 Policy Development

Finally, legal frameworks must recognize that one-size-fits-all regulation will not suffice. Policymakers should:

- Engage with cultural advisors and anthropologists when drafting digital estate laws
- Recognize traditional inheritance patterns and family structures
- Provide flexible templates that allow for culturally specific expressions of consent and delegation
- Ensure protections are in place for users in non-dominant or marginalized communities, whose digital lives may not fit normative patterns

Incorporating cultural nuance into digital estate policy is not just a matter of fairness. It is essential for ensuring that systems built to manage identity, memory, and legacy reflect the full range of human experience (Desert Law Group, 2023).<sup>22</sup>

# 3 Who and What Is at Risk

Despite growing awareness of the persistence of digital assets after death, most systems today remain unprepared for what happens next. Families, executors, and dependents are left to navigate closed platforms, incomplete laws, and technical gaps, often while grieving. This section lays out what’s at stake when digital estate planning is absent or inadequate.

## 3.1 Emotional Cost

For many families, grief is compounded by digital inaccessibility. Bereaved individuals find themselves locked out of accounts containing photos, messages, or records of connection, unable to retrieve even the smallest traces of their loved one’s presence. In other cases, algorithms surface unwanted reminders without consent: birthday notifications, tagged

---

<sup>21</sup> Society of Trust and Estate Practitioners. “Protect Your Digital Memories Campaign Toolkit.” <https://www.step.org/digital-assets/protect-your-digital-memories-campaign-toolkit>.

<sup>22</sup> Desert Law Group. “Incorporating Cultural Beliefs into Your Estate Planning.” <https://desertlawgroup.com/blog/cultural-beliefs/incorporating-cultural-beliefs-into-your-estate-planning/>.

photos, or AI-generated content of the deceased. These uninvited interactions can retraumatize, creating a cycle of digital hauntings instead of closure.

Worse, in some systems, there is no clear way to delete an account posthumously. Survivors are forced to interact with a digital ghost they can neither control nor lay to rest.

## 3.2 Financial Risk

Digital estates increasingly carry financial value. As Beyer and Nipp detail,<sup>23</sup> they may include:

- Cryptocurrency wallets (often unrecoverable without the private key)
- Domain names (with revenue potential or brand value)
- Monetized content accounts (e.g., YouTube, Substack, Etsy)
- Unspent loyalty points and digital gift cards
- Cloud storage tied to paid plans, which may contain valuable or legally significant files

Without access, these assets may be lost forever or fall into the wrong hands. Fiduciaries face legal and logistical challenges when credentials are unavailable and platforms lack protocols for verified handover.

Digital estates may also include:

- Online-only bank and financial accounts (often impossible to discover during probate)
- Metaverse assets (which may require access to such Metaverse and know-how to recoup)
- Email accounts, which may contain valuable records or legally significant information

## 3.3 Abuse, Exploitation, and Fraud

Digital legacies are not immune to misuse. In the absence of protections:

- Deepfakes can simulate a dead person's voice or likeness for manipulation, disinformation, or profit.
- Impersonation can be used in social engineering or scams, either targeting survivors or using the deceased as bait.
- Stalking or emotional abuse may occur when abusers weaponize access to shared accounts, photos, or metadata.
- Personal data collected by websites, including purchases, chats, and any information submitted electronically, loses all protection under the GDPR and CCPA

---

<sup>23</sup> Gerry W. Beyer and Kerri Nipp, "Estate Planning for Cyber Property, Electronic Communications, Cryptocurrency, Non-Fungible Tokens, and the Metaverse," *Estate Planning & Community Property Law Journal* 16, no. 1 (2023), <https://epj.us/volume-16>.

upon death (Stamp 2024).<sup>24</sup> Cohen's work on posthumous harm argues that identity autonomy does not end at death, and failure to protect it opens space for abuse, not only of memory, but of power.

### 3.4 Loss of Identity Autonomy

A person's online presence is not just a set of logins; it is a narrative. Without pre-defined choices, a person's digital legacy may be deleted, rewritten, or exploited in ways they never intended. This is especially urgent in:

- Suicide cases, where intent around the digital afterlife may be complex
- Estranged family dynamics, where next-of-kin may act against a person's values or wishes
- Cultural or religious contexts, where memorialization must be handled carefully

As AI avatars become more realistic, the risk of being "reanimated" against one's wishes continues to grow.

### 3.5 Special Populations at Heightened Risk

Some groups face disproportionate harm from the lack of digital estate protections:

- Minors: As Banta highlights, children accumulate digital assets without the legal tools to manage or assign them. Upon death, their data is often handled entirely by parents or platforms, with little regard for autonomy.
- Marginalized communities: For LGBTQ+ individuals or political dissidents, online history may contain sensitive identity markers. Posthumous exposure can endanger reputations, communities, or the remaining family.
- High-profile individuals: Public figures' accounts are prone to hijacking, unauthorized memorialization, or posthumous branding, turning legacy into spectacle.

### 3.6 Public Awareness is Low

Even in highly connected societies, digital death planning remains rare. In Japan, as mentioned, the government has urged citizens to share their passwords in wills or digital notebooks to avoid chaos, but uptake has been limited. The gap between risk and readiness remains vast, even when governments try to raise awareness.

Without explicit, user-driven mechanisms for digital estate planning, we risk emotional harm, financial loss, identity misuse, and systemic erasure. The urgency is real and growing.

---

<sup>24</sup> Niall Stamp, "GDPR and Personal Data After Death - GDPR EU," GDPR EU, October 25, 2024, <https://www.gdpreu.org/gdpr-faqs/gdpr-and-personal-data-after-death/>.

## 4 Legal and Regulatory Touchpoints

As our lives migrate online, the systems governing death, incapacitation, and delegation struggle to keep pace. Legal frameworks were not designed with digital legacies in mind, and where new laws have emerged, they often lack consistency or clarity. This section outlines the existing scaffolding; what works, where it falls short, and why uniform policy remains elusive.

### 4.1 A Patchwork of Protections

In the United States, the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) was adopted to provide a legal pathway for fiduciaries, such as executors or guardians, to access a person's digital assets.<sup>25</sup> RUFADAA establishes a tiered hierarchy for access:

1. Online tools provided by the platform (such as Google's Inactive Account Manager) take precedence,
2. Followed by instructions in the estate plan (such as a will, power of attorney (POA), and trust agreement),
3. And finally, the platform's terms of service (ToS) fill in the gaps.

While this model attempts to balance user intent with platform control, it often defaults to the ToS in practice. Most users never configure online tools (if they exist) or specify digital wishes in their estate plans because they are unaware of the need to plan in this area. Additionally, platform providers often fail to draw user attention to these features, which are frequently buried in hard-to-find corners of platform settings. As a result, the default ToS—written unilaterally by platforms—becomes the de facto rule. These vary wildly, are often vague or restrictive, and are not designed to accommodate the complexity of grief, incapacity, fiduciary roles, or long-term digital preservation.<sup>26</sup>

Furthermore, if a platform offers an online tool, most users do not consider the potential tensions and issues that may arise. If a user selects a designated recipient through the online tool who differs from the legal representative of the user's estate, complications may follow. The legal representative may be unable to obtain information given to the designated recipient. That information may be required for proper estate administration or may have tax or other consequences for the estate. The concept of an online tool is very similar to a beneficiary designation on a traditional asset without the well settled law to invalidate such designations in a variety of situations (i.e., divorce, death of the named recipient, or inaccurate contact information provided for the designated recipient, etc.) and such selections should be done with care and as part of an overall estate plan.

---

<sup>25</sup> "Fiduciary Access to Digital Assets Act, Revised."

<sup>26</sup> Queen Mary University in partnership with Microsoft cloud project did a survey on Terms of Service and found most do not address death/incapacity. ("Cloud Contracts - Cloud Legal Project" n.d.)

## 4.2 Jurisdictional Silos and Systemic Gaps

U.S. law remains fragmented. While RUFADAA has been adopted in most states, right of publicity laws, which govern how a person's likeness can be used after death, are entirely state-based and often inconsistent. In some jurisdictions, the right of publicity ends at death. In others, it extends for decades. There is no coherent national policy for posthumous digital presence or identity protection.

Worse, minors are often left out of the equation entirely. As Banta notes, children may accumulate significant digital content—such as social media, gaming profiles, and school files—without ever having the legal standing to determine its future. Parents or guardians may act on their behalf, but there are few safeguards to ensure that the minor's preferences or privacy are respected posthumously.

## 4.3 International Signals, but Global Incoherence

Globally, the picture is even more varied. In Japan, government guidance encourages citizens to store their digital credentials in wills or written documents to avoid family confusion and legal conflict. But this is advice, not policy, and uptake remains low. Furthermore, not all credentials may be stored in these documents, as the industry is shifting away from knowledge-based credentials, such as passwords. Other countries, particularly those with strong data protection regimes, face additional hurdles: How does the right to be forgotten intersect with the concept of death? Who has the authority to request deletion or preservation?

There is no international convention for digital estate access, fiduciary identity, or posthumous data governance. Multinational platforms navigate this complexity inconsistently, often prioritizing compliance by region over coherence by design.

## 4.4 Global Landscape: Digital Estate Planning by Region

As digital legacies proliferate across every region of the world, governments and legal communities are grappling with how to treat digital assets after the death of their owners. Some countries are moving toward clear statutory definitions and inheritance rules, while others rely on older frameworks that did not anticipate online accounts, encrypted data, or virtual property. The following overview offers examples of how different regions are approaching digital estate planning.

#### 4.4.1 United Kingdom

The UK is progressing towards formal recognition of digital assets in estate planning. The proposed Property (Digital Assets, etc.) Bill aims to classify digital assets as personal property, ensuring they are included in wills and subject to inheritance laws.<sup>27</sup>

#### 4.4.2 Japan

Japan currently lacks specific legislation governing the inheritance of digital assets. However, public awareness is increasing, with surveys indicating a growing desire among citizens to proactively manage their digital legacies.<sup>28</sup>

#### 4.4.3 Australia

Australia does not have comprehensive laws addressing digital assets in estate planning. This absence creates challenges for executors, who may face difficulties accessing online accounts due to privacy laws and service agreements.

#### 4.4.4 India

India's legal framework does not currently recognize digital assets in estate planning. Nonetheless, a growing movement is advocating for the inclusion of digital assets in wills and the formalization of roles such as digital executors.

#### 4.4.5 European Union

The European Law Institute is working on harmonizing laws related to digital asset succession across member states. Their project aims to define digital remains and establish clear guidelines for their inheritance and data protection.<sup>29</sup>

#### 4.4.6 South Africa: Legal Foundations and Emerging Practices

South Africa is among the more advanced African nations in integrating digital assets into estate planning. While digital assets are not yet explicitly defined in law, existing legislation provides a framework:

---

<sup>27</sup> UK Parliament, "Property (Digital Assets etc) Act 2025," December 3, 2025, <https://bills.parliament.uk/bills/3766>.

<sup>28</sup> Atsushi ISEDA, "Manual for Handling Digital Assets Left by the Deceased," *New Breeze*, season-02 2020, [https://www.ituaj.jp/wp-content/uploads/2020/07/nb32-3\\_web\\_1\\_Special\\_ManualDigitalAssets.pdf](https://www.ituaj.jp/wp-content/uploads/2020/07/nb32-3_web_1_Special_ManualDigitalAssets.pdf).

<sup>29</sup> "ELI Succession of Digital Assets, Data and Other Digital Remains," n.d., <https://www.europeanlawinstitute.eu/projects-instruments/current-projects/current-projects/eli-succession-of-digital-assets-data-and-other-digital-remains/>.

- **Intestate Succession Act 81 of 1987:** Governs the administration of deceased estates, including digital assets.<sup>30</sup>
- **Electronic Communications and Transactions Act (2002):** Addresses electronic transactions and may apply to digital assets.
- **Protection of Personal Information Act (2013):** Regulates the processing of personal information, relevant to digital assets containing personal data

Estate planning professionals recommend creating a digital asset inventory, including login credentials, and appointing a digital executor to manage these assets posthumously.

#### 4.4.7 Nigeria: Navigating Legal Ambiguities

In Nigeria, the legal framework for digital asset inheritance remains underdeveloped. Traditional probate laws do not explicitly address digital assets, resulting in uncertainties regarding their management and transfer upon death. Legal experts advocate for updating probate and inheritance laws to recognize digital assets, ensuring they can be effectively managed and passed on to heirs.<sup>31</sup>

#### 4.4.8 Tanzania: Calls for Legal Frameworks

In Tanzania, there is a growing recognition of the need for legal frameworks to manage digital assets after death. Experts emphasize the importance of educating the public on digital asset management and integrating digital inheritance practices into existing legal systems to protect individuals' digital legacies.<sup>32</sup>

#### 4.4.9 Other Regional Initiatives in Africa: Pollicy's "Mine is Yours" Project

The civic technology organization Pollicy has launched the "Mine is Yours" project (Magege and Saturday, "Mine Is Yours - Pollicy"), focusing on digital asset management and inheritance in Africa, with pilot studies in Malawi, Ghana, and Tanzania.<sup>33</sup> The project aims to:

- Raise awareness about digital assets and their importance in estate planning.
- Encourage the inclusion of digital assets in wills.
- Advocate for legal reforms to accommodate digital inheritance.

---

<sup>30</sup> "Intestate Succession Act 81 of 1987 | South African Government," March 18, 1988, <https://www.gov.za/documents/intestate-succession-act-10-mar-2015-1416>.

<sup>31</sup> Ayoyinka Olajide-Awosedo, "Navigating the Legal Grey Areas of Digital Assets in Nigeria - Global Law Experts," *Global Law Experts*, June 6, 2025, <https://globallawexperts.com/navigating-the-legal-grey-areas-of-digital-assets-in-nigeria/>.

<sup>32</sup> Site unavailable as of 17 December 2025: <https://dailynews.co.tz/digital-assets-digital-legacies-the-future-of-inheritance/>

<sup>33</sup> Rachel Magege and Bonaventure Saturday, "Mine Is Yours - Pollicy," *Pollicy*, April 30, 2025, <https://pollicy.org/resource/mine-is-yours/>.

This initiative highlights the need for a comprehensive approach to digital inheritance, considering the continent's rapid technological adoption.

## 4.5 Industry Approaches to Digital Asset Estate Planning

As individuals accumulate more financial, social, and personal assets online, industry sectors are adapting their practices to support digital estate planning. Banks, investment firms, and technology companies are introducing tools, guidance, and account-management features designed to help individuals document and transfer their digital assets after death. These approaches vary widely, reflecting both growing demand and the practical limits of what service providers can make available to heirs or executors.

### 4.5.1 Financial Services

Financial institutions are increasingly recognizing the importance of digital assets in estate planning. Firms like Fidelity and Merrill Lynch offer guidance on incorporating digital assets into estate plans, emphasizing the need for detailed inventories and clear directives.

### 4.5.2 Technology Sector

Tech companies are developing tools to help users manage their digital legacies. For instance, Apple and Facebook offer features that allow users to designate legacy contacts who can manage their accounts after they pass away.<sup>34</sup> However, service providers can, and do, limit what data may be accessed posthumously. Apple, for example, does not allow legacy contacts to access credentials stored in Apple's Passwords application. This restricts the ability of the legacy contact to discover and manage the deceased's online accounts.

This global and industry-specific overview highlights the evolving nature of digital estate planning. As digital assets become increasingly integral to our lives, the need for clear legal frameworks and proactive planning becomes ever more critical.

### 4.5.3 Healthcare Industry

The healthcare industry is increasingly recognizing that digital identities and records extend beyond life and that planning for them should be part of end-of-life care discussions. Professional guidance emphasizes creating a digital inventory, specifying a trusted person (often aligned with the health-care or estate executor) to manage or shut down online accounts, and embedding those instructions in advance-care or estate-planning documents. While many hospitals and hospice organizations encourage patients and their families to consider physical assets, fewer explicitly address the continuity of digital assets. The result is that caregivers sometimes struggle to access the necessary information

---

<sup>34</sup> Mark Sellman, "Digital Will' Services Let Loved Ones Access Social Media Accounts," *The Times*, August 12, 2024, <https://www.thetimes.com/uk/technology-uk/article/digital-will-services-let-loved-ones-access-social-media-accounts-g5qvqtt60>.

because service providers block access without proper legal permission. Given the sensitivity of health data, message exchange and hosting platforms may require both regulatory compliance (HIPAA-type rules) and platform-specific policies. Care providers and patients alike are advised to combine digital asset instructions with clear authorizations and periodic reviews.

## 5 The Technology Landscape

In theory, we live in an age where digital estates and access to data can be flexibly delegated, revoked, and inherited. In practice, the technical tools to manage digital estates are inconsistent, incomplete, and largely proprietary. This leaves us with a mixed set of incomplete tools to manage their digital assets.

### 5.1 Fragmented Tooling and Uneven Coverage

Some major platforms have taken steps to acknowledge the reality of death in their user base. Facebook's [Legacy Contact](#) and Google's [Inactive Account Manager](#) are two of the more mature tools available. They allow users to pre-designate someone to manage or delete their account after death or prolonged inactivity. These features, however, are platform-specific, opaque in behavior, and have limitations. A legacy contact can pin a post or update a profile picture, but they cannot read messages or access all data. Meanwhile, smaller platforms do not offer delegation capabilities at all, leaving families and fiduciaries to navigate support tickets, Terms of Service clauses, or court orders.

Of more concern is the increasing centralization of credentials within credential managers, a category that now includes both traditional password vaults and emerging digital wallets. As major platforms promote passkeys and other phishing-resistant authentication methods, users are increasingly relying on credential managers rather than memorized (and often reused) passwords. This shift significantly improves usability and security, but it also changes how—and whether—credentials are visible or accessible to anyone acting on a user's behalf. Credentials stored in password vaults or bound to devices and wallets may not be readily discoverable by an estate manager or fiduciary, particularly when access depends on possession of specific hardware, biometric factors, or platform-controlled recovery flows.

Some credential managers, particularly password-management services such as [1Password](#), [LastPass](#), and [Bitwarden](#) offer “emergency access” or “designated access” features that allow users to grant trusted individuals conditional access to their vaults. These mechanisms can mitigate estate-access challenges, but only if they are explicitly configured during the user's lifetime. Digital wallets, by contrast, often lack equivalent estate-planning features and may rely on platform-level account recovery processes that are opaque or tightly constrained. Without proactive preparation, estate managers may be

forced to pursue recovery on an account-by-account basis, a time-consuming effort that may ultimately fail, leaving some accounts inaccessible and unmanaged.

In an environment of inconsistent approaches for digital estate management, the industry has failed to deliver tools to effectively manage users' digital estates upon death and incapacitation. There are no standardized technical models for managing the state transition from an active account to one being managed as part of a digital estate, nor do we have suitable technical models to express the delegated authority required for digital estates.

## 5.2 Where Technical Models *Do* Exist

Some technical communities have begun to address the complexities of posthumous or proxy identity. The Sovrin guardianship credentials model (Sovrin Foundation, "Guardianship"), developed in the context of self-sovereign identity (SSI), offers a compelling starting point.<sup>35</sup> It clearly distinguishes between dependent and guardian roles, includes legal jurisdictional anchoring, supports revocability, and ensures auditability. Sovrin's layered approach (governance, define-time, and run-time) shows how a delegated relationship can evolve over time without sacrificing privacy or control. While initially designed for health and aging use cases, the design could also be extended to death and digital legacy scenarios.

Similarly, Kantara's UMA project has spent years exploring consent, delegation, and relationship management.<sup>36</sup> Their legal subgroup's notes highlight the importance of capturing user intent, especially in non-binary scenarios such as co-equal authority or evolving capacity. UMA's framework supports multi-party delegation, bounded access scopes, and time-limited roles. It is one of the few models that directly considers the ambiguity of "family" and the risk of overlapping authority (such as during divorce, estrangement, care transitions, or contested estates).

In parallel, the OpenID Foundation's eKYC and Identity Assurance Working Group is developing a *Delegated Authority Specification for Digital Trust*, which aims to standardize the verification, assignment, management, and revocation of delegated authority across digital systems.<sup>37</sup> Unlike earlier models focused primarily on human-to-human delegation, this work explicitly encompasses humans and AI agents acting on behalf of others, including individuals, organizations, and automated systems. Its scope spans online services, SaaS platforms, healthcare, and business process automation, reflecting the growing need for durable, auditable delegation mechanisms that operate across domains and lifecycles. While not specific to posthumous identity, the specification provides a foundational

---

<sup>35</sup> Sovrin Foundation, "Guardianship," Sovrin, May 28, 2023, <https://sovrin.org/guardianship/>.

<sup>36</sup> Kantara Initiative, "User-Managed Access."

<sup>37</sup> OpenID Foundation, "eKYC & IDA Working Group - OpenID Foundation," OpenID Foundation - Helping People Assert Their Identity Wherever They Choose, January 23, 2025, <https://openid.net/wg/ekyc-ida/>.

framework for representing authority relationships that can adapt over time, an essential prerequisite for addressing proxy, guardianship, and estate-related use cases in complex digital environments.

Finally, legal experts such as Beyer and Nipp have detailed how estate planning practices are evolving to keep up with digital complexity (Beyer and Nipp, “Estate Planning for Cyber Property, Electronic Communications, Cryptocurrency, Non-Fungible Tokens, and the Metaverse”).<sup>38</sup> Their work shows the diverse range of assets (from blogs and NFTs to cloud accounts and encrypted drives) and the absence of consistent technical tools to locate, authorize, or preserve those assets posthumously.

---

<sup>38</sup> Beyer and Nipp, “Estate Planning for Cyber Property, Electronic Communications, Cryptocurrency, Non-Fungible Tokens, and the Metaverse.”

### THE UNFINISHED DIGITAL ESTATE LIFECYCLE: LESSONS FROM NATIONAL ID SYSTEMS

MOSIP positions itself as a national identity platform designed to provide a reliable, interoperable foundation for national ID systems that governments can adopt and adapt.<sup>39</sup> In particular, MOSIP's role in managing the end of life is focused on integrating with civil registration systems to record declarations of death and make that information accessible to relying parties that have previously completed KYC checks.

This approach ensures that service providers (for example, banks or social networks) can confirm the death of an individual through a legally accurate source. Certain entities, pre-approved by law, may even receive direct notifications. However, MOSIP draws a clear line: delegation, transfer of access, and inheritance of digital accounts are not handled by the national ID platform. Those processes remain the responsibility of nominees and individual service providers, governed by local regulation and business policy.

MOSIP also recognizes the practical complexity of this space. A death notice is not always permanent: it can be revoked if circumstances change, and systems like tax authorities may still require access to the identity record long after the individual's death. Fraud risks—from faked deaths to unreported deaths, nominee manipulation, or judicially declared deaths—further highlight why digital estate management cannot rest solely with a national identity system.

What emerges is a missing concept of the digital estate lifecycle. While MOSIP can provide accurate declarations of death, it does not—and arguably cannot—go further in defining how digital assets, permissions, and identities should be transferred or unwound. That lifecycle requires coordination across government, industry, and civil society. Without such a shared model, the risk of fraud, disputes, and unmanaged digital legacies will persist.

## 5.3 The Interoperability Gap

Despite these efforts, no widely adopted framework currently ties identity delegation to estate events, such as death or incapacitation. We lack standardized:

- Mechanisms to express delegated access rights (and state change events of the data owner, e.g., incapacitation notices, digital death certificates, assignment of executor, etc.
- Consistent, trustworthy APIs for requesting and verifying death or incapacitation status, and mechanisms to revoke the same if an error has occurred

---

<sup>39</sup> MOSIP, "MOSIP," accessed December 17, 2025, <https://www.mosip.io/>.

- Delegation protocols that work across identity providers and platforms, where delegation is contingent upon the data owner's death or incapacitation

Without these, even well-intentioned estate planning falls apart in execution. A user might assign a digital fiduciary in their will, but if the service provider doesn't recognize it or lacks the tools to validate and act on it, nothing happens. Or worse, irreversible deletion happens anyway. If a digital fiduciary is appointed in the will but is unable or unwilling to fulfill their duties on behalf of the deceased, the digital estate may be left in an unknown, unowned, and unmanaged state. Finally, the digital fiduciary may not be aware of all of the services that hold the deceased's digital data. These services may not be easily discoverable, leaving a subset of the deceased's assets unmanaged and, effectively, unowned and orphaned.

When the account owner is affected by an event such as death or incapacitation, service providers must be able to obtain notice of the state change, thereby enabling the user's chosen individuals to access and manage their digital assets in accordance with the service provider's rules and regulations. At the time of writing, there is no defined protocol or mechanism to enable such interactions. The OpenID Foundation is well-positioned to design such protocols, potentially by extending existing protocols, with the cooperation of service providers, governments, lawyers, and experts in identity systems.

## 5.4 A Path Forward

Digital estate planning will not be viable at scale until the technical stack supports delegation that is verifiable, revocable, interoperable, and usable by the average person with or without legal representation. Service providers, such as social media sites, cloud services, and online crypto wallets, require *digital estate services* to manage their users' *legacy managers*.

Digital estate services must operate as trusted intermediaries for service providers to bridge the gap between their users and legacy managers, while providing privacy guarantees to the estate owner and protecting against the abuse of these tools for account hijacking. This is accomplished by limiting the data shared with service providers to the existence of the estate and how to identify the legacy managers for the user's estate.

The legacy manager is a designated individual (or individuals) who is assigned rights over the user's estate. Legacy managers may receive specific instructions (e.g., "Please delete my blog and all social media accounts 5 years after my death") in a manner consistent with traditional estate planning. In addition, the legacy managers receive credentials that are used to access the estate owner's data at service providers that have been registered with the digital estate service. However, these credentials must only be issued by the digital estate service upon confirmation of the estate owner's death or incapacitation, as defined in their estate plan.

The legacy manager credentials are issued to the legacy managers after sufficient identity proofing of the legacy manager and verification of their delegated rights and

responsibilities, along with instructions on how to use the credentials at the list of registered services. Service providers, upon receiving a credential from a legacy manager, validate the credential and provide access to the owner's digital assets held at the service provider. The specific data the legacy manager is authorized to access is dependent on the service provider's terms of service. In some cases, the legacy manager may be able to impersonate the owner, while other service providers may limit the data accessible to the legacy manager and even require termination of the account once any assets have been recovered. Given the innumerable scenarios possible, service providers are expected to define their own policies and optionally allow users specific choices about how their data and accounts may be handled by legacy managers.

By enabling a distributed protocol to allow assignment of legacy managers that is independent of the data authorization at service providers, this mechanism remains scalable, allowing service providers the flexibility to enable digital estate management tools in the manner that best serves their user community without the complexity of having to manage legacy manager identities or validate government documents such as death certificates. The processes for obtaining and validating death certificates, onboarding and identity proofing of legacy managers, and operating the digital estate services must be governed by appropriate trust frameworks designed to work across regions and jurisdictions.

While these cultural perspectives illustrate the diversity of ways societies view death and legacy, they also shape legal defaults about who may act on behalf of the deceased or incapacitated. The next section examines how these cultural expectations are encoded into law—particularly through guardianship, inheritance, and fiduciary access—and what this means for family authority in digital estate management.

## 6 Delegation, Guardianship, and Identity Transitions

Digital estate planning is not just a matter of asset transfer. It is about delegating identity, authority, and agency in ways that can be misused if not carefully structured. Effective delegation must distinguish between acting *as* someone else and acting *on behalf of* someone else, with mechanisms that preserve autonomy, enforce consent, and withstand scrutiny. This section explores the semantics, standards, threat models, and mitigation strategies for secure and ethical delegation. Services should select the mechanisms that are most suitable for their unique use cases.

## 6.1 Delegation Semantics: Impersonation vs. Acting on Behalf Of

At the core of digital delegation is a semantic tension: is the delegate impersonating the user, or are they acting with limited authority on their behalf? Impersonation often involves full credential access, which collapses identity boundaries and obscures accountability. True "on-behalf-of" delegation, by contrast, maintains the identity distinction between principal and agent. It supports role clarity, scope limitation, revocability, and accountability.

In physical life, proxies and powers of attorney fill this function. Online, most systems do not distinguish between a person and their credentials, leaving no room for structured delegation that aligns with legal or ethical norms.

In practice, impersonation is often employed by many services due to the limited availability of alternative options. In other cases, the Terms of Service stipulate that posthumous impersonation of the account owner is prohibited, including the possession of their credentials. When planning a digital estate, individuals are encouraged to share their credentials in various ways, such as writing them down or sharing them to unlock a password manager. Credential sharing directly supports impersonation and is easy for the service provider to implement; no changes are required. However, this can lead to unintended consequences, such as a deceased individual's account being used to post on social media.<sup>40</sup> To minimize such undesirable outcomes, services must consider how to deploy on-behalf-of delegation models for legacy managers and deprecate impersonation-based processes.

Enabling legacy managers to act on behalf of the data owner is more challenging; however, it has been implemented by organizations such as Apple, which provides a mechanism to enable a legacy manager and provides the legacy manager with a unique credential to access some, but not all, of the principal's data. While this model is more flexible, the industry has not coalesced around standards that allow for the expression of a wide variety of delegation semantics, including time-bound delegation, re-delegation, and contingent delegation (e.g., delegation upon a triggering event, such as reaching the age of maturity).

## 6.2 Technical Basis: Tokens and Transitions

The OAuth 2.0 Token Exchange specification (RFC 8693) provides a starting point for token-based delegation.<sup>41</sup> It allows one security token to be exchanged for another with an

---

<sup>40</sup> Andrew Solender, "Dead congressman promotes candidate for his seat on social media," Axios, June 24, 2025, accessed December 17, 2025, <https://www.axios.com/2025/06/24/gerry-connolly-james-walkinshaw-dead-social-media>.

<sup>41</sup> Mike Jones, Anthony Nadalin, Brian Campbell, Ed., John Bradley, and Chuck Mortimore, "OAuth 2.0 Token Exchange", RFC 8693, DOI 10.17487/RFC8693, January 2020, <<https://www.rfc-editor.org/info/rfc8693>>.

altered scope or subject context, enabling on-behalf-of semantics in identity and access management. These tokens can encode metadata for:

- Actor tokens: indicating that one identity is acting for another
- Role transitions: such as caregiver, executor, or fiduciary
- Scope and duration: allowing granular control over what can be done, and for how long
- Revocation and auditability: enabling retrospective verification and timely withdrawal of access

However, implementation is uneven. Most platforms treat delegation as an edge case or rely on informal, out-of-band processes, such as emailed screenshots or password sharing.

## 6.3 Evolving Models for Guardianship and Shared Authority

Forward-looking initiatives are beginning to formalize digital guardianship. For example:

- Sovrin's guardianship framework defines layered roles (e.g., guardian, observer, delegate) with embedded legal scope, revocation capabilities, and audit mechanisms. It emphasizes verifiable delegation, where guardianship claims are tied to cryptographic proofs and subject to challenge.
- Kantara's UMA working group has examined the role of co-equal Resource Rights Administrator (RRAs), supporting scenarios where shared access must reflect intent, not just authority. Their work proposes delegation that is:
  - Explicitly consented
  - Time-bound and purpose-scoped
  - Transparent to the user

These models seek to operationalize trust without collapsing the identity of the delegator and delegate, a critical requirement for systems that support transitions during incapacity or after death.

## 6.4 Cultural Norms in Law and Family Authority

Family authority over digital estates does not arise solely from tradition; in many jurisdictions, it is explicitly written into law. Statutes on inheritance, guardianship, and fiduciary access often presume that next of kin should manage a deceased or incapacitated person's accounts. While this approach aligns with cultural expectations in many collectivist societies, where filial duty or extended family rights are paramount, it can clash with individualist traditions that prioritize personal autonomy and explicit consent.

These legal defaults create both opportunities and risks. On one hand, they provide continuity and prevent digital assets from becoming stranded. On the other, they may override the wishes of the account holder or enable coercion within families. For example, guardianship laws designed to protect elders can be misused for financial exploitation,

while statutory inheritance rules may give family members access to communications the deceased never intended to share.

The challenge for digital estate management is that cultural norms are not uniform, yet laws often enforce a single model of authority. Systems built on these defaults risk imposing culturally narrow assumptions, treating kinship as a universal proxy for consent. Effective safeguards must therefore recognize that family authority is both culturally variable and legally constructed, requiring technical protocols that can reflect individual intent without dismissing collective traditions.

## 6.5 Delegation Threat Models and Abuse Scenarios

Delegation is not a neutral act. While the ability to act on someone else's behalf is essential for managing digital estates, it also introduces new vectors for abuse. Authority rarely exists in a vacuum; it sits within cultural norms, family dynamics, and institutional hierarchies. Power imbalances, coercion, and institutional authority can all distort the intent of delegation, turning a protective measure into a tool of harm. These risks are not theoretical; they mirror patterns already seen in elder exploitation, domestic abuse, and misuse of guardianship in physical life. Digital systems often amplify those patterns by stripping away context and reducing relationships to credentials, permissions, or cryptographic proofs.

To design digital estate systems that are both trustworthy and humane, we must anticipate the most common scenarios where delegation can be misused. The following subsections outline four of the most pressing: elder financial exploitation, partner and domestic abuse, institutional overreach, and inheritance without intent. Each illustrates how fragile digital identity becomes when authority is assumed, coerced, or automated without safeguards. We will discuss recommendations to mitigate these threats in Section 8.

### 6.5.1 Elder Abuse and Financial Exploitation

Older adults often face pressure to hand over digital access to caregivers or relatives. When credentials become the only means of delegation, that pressure can turn into exploitation, such as draining accounts, redirecting benefits, or erasing autonomy. Cultural traditions that value filial responsibility can intensify this pressure, making resistance socially unacceptable even when abuse is suspected. Without verifiable delegation models and audit trails, systems make it easy for abusers to act invisibly.

### 6.5.2 Partner and Domestic Abuse

Delegation can also be weaponized within intimate relationships. Abusive partners may demand credentials, manipulate shared accounts, or coerce access as a form of control. In these cases, digital identity becomes a tool for isolation or intimidation. Legal remedies are often slow or inaccessible, leaving technical safeguards as the first line of defense. Systems

that lack revocation and monitoring features leave victims with no meaningful way to reassert control.

### 6.5.3 Institutional Overreach

Beyond families, institutions that manage minors or vulnerable adults (e.g., schools, group homes, or religious organizations) may claim delegated authority over digital accounts. Even where such oversight is motivated by care or protection, unchecked control can slip into surveillance, ideological enforcement, or silent erasure of a person's digital presence. Safeguards must prevent institutional control from overriding user intent.

### 6.5.4 Inheritance Without Intent

Finally, defaulting authority to next of kin can erase the wishes of the deceased. Automatic access may lead to premature deletion, suppression of sensitive history, or contested ownership of digital assets. Inheritance laws vary significantly across cultures, with some prioritizing individual autonomy and others emphasizing collective family rights. Digital systems risk flattening those differences, imposing one-size-fits-all defaults that undermine both privacy and tradition.

## 7 Posthumous AI and the Question of Digital Humanity

### 7.1 Persistence Through Synthetic Media

AI, specifically generative AI (GenAI), is changing the way humans perceive and relate to death. It is creating new options for both the dying and the bereaved and raising new questions about what it means to be digitally human.

These new concerns are raised succinctly in the story of a young Canadian man named Joshua.<sup>42</sup> His girlfriend, Jessica, had a long-term illness. She died at the age of 23, and even eight years later, he had not gotten over her tragic passing. This occurred in 2020, during the early days of GenAI. He signed up for a service that created chatbots, and then fed it the texts and emails that he had received from her over the years.

He started up the bot, and it acted and sounded like Jessica. For over a year, he talked to the "new Jessica" as if it were her, including discussing her own death. Was this act of creation right or wrong?

---

<sup>42</sup> Jason Fagone, "The Jessica Simulation: Love and loss in the age of A.I.," *The San Francisco Chronicle*, July 23, 2021, <https://www.sfchronicle.com/projects/2021/jessica-simulation-artificial-intelligence/>.

You can argue both ways: on one hand, it helped him grieve, process, and say goodbye. However, on the other hand, the only reason he said goodbye to the “new Jessica” was that there was a strict time limit on how long the bot could continue to exist.

Such options did not exist prior to the advent of GenAI. And while it was once merely chatbots that were being created to emulate the deceased, full audio and video recreations are now possible.

Services are coming online with a wide range of potential offerings. Some, such as [StoryFile](#), aim to preserve their stories and memories for both the general public and their close friends and family. Others ([HereAfter](#)) market themselves to people so that they can preserve their own legacy and stories for their loved ones.

This technological capability is not limited to the personal sphere either, as replicas may be generated based on a very short video/audio clip of the person. This puts well-known figures or celebrities into play.

Past historical figures are being recreated by groups such as [Hello History](#), and current celebrities are facing a wide range of deepfakes that are generated without their permission. For example, in 2024, Scarlett Johansson was approached by OpenAI to be the voice of their ChatGPT 4.0 bot. She declined, but the company released a voice that was “indistinguishable from her own.”<sup>43</sup> After threatening legal action, the company retracted this offering.

Ms. Johansson is not alone. Brad Pitt, Tom Hanks, and Taylor Swift, along with a host of other well-known celebrities and public figures, have been recreated by GenAI for financial and political purposes.

## 7.2 Consent and Control

The legal control of digital representation after death is a complex issue that continues to be debated in both the courts and the public sphere. Clearly, the individual should retain rights over their likeness while they are alive, but how can (or should) this authority be transferred after death?

A few recent experiences highlight the significant questions that AI technology presents:

- In Arizona, a man slain in a road rage incident was recreated by AI and allowed to deliver a statement during the sentencing of the man who killed him.<sup>44</sup>

---

<sup>43</sup> “OpenAI’s use of Scarlett Johansson-like voice in ChatGPT exposed gaps in the law,” American Bar Association, November 21, 2024, accessed December 17, 2025, [https://www.americanbar.org/advocacy/governmental\\_legislative\\_work/publications/washingtonletter/november-24-wl/openai-scarlett-johansson-1124wl/](https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/november-24-wl/openai-scarlett-johansson-1124wl/).

<sup>44</sup> Juliana Kim, “Family Shows AI Video of Slain Victim as an Impact Statement — Possibly a Legal First,” *NPR*, May 12, 2025, <https://www.npr.org/2025/05/07/g-s1-64640/ai-impact-statement-murder-victim>.

- Former CNN White House correspondent Jim Acosta “interviewed” an AI-generated avatar that recreated Joaquin Oliver, a teenager killed in the 2018 Parkland high school shooting.<sup>45</sup>

These recreations highlight the potential for a deceased person’s likeness to be used without their explicit permission (or even their awareness that such a thing was possible). In these cases, it would seem that the words expressed by the deceased were crafted by the creators of the avatars rather than the individual themselves. Even if the deceased might agree with the statements expressed by the recreation, they are still not “authentic.” In a world where what is seen and heard has been believed, that may present problems for the veracity of any and all videos (even if they are not created by AI).

The authority over the likeness of the deceased presents additional challenges. If there are unauthorized AI representations, how are the authorized guardians equipped to restrict or prevent rogue uses of the deceased’s likenesses? In addition, are there boundary lines that need to exist based on fair use of a public figure’s imagery or questions of copyright timelines?

## 7.3 Legal and Ethical Questions

These questions fall in line with the recent concerns of personal data, the right-to-be-forgotten, and other forms of privacy legislation (GDPR, CDPA, PDPA, etc.). This has been recognized by several legislative bodies, with varying degrees of success and progress.

The European Union recently passed the EU AI Act, which begins to provide some safeguards in the use of GenAI.<sup>46</sup> In February of 2025, bans on unacceptable-risk practices, including deepfakes without consent, came into force. Over time, additional rules for transparency and clear demarcation of AI-generated content may help address the higher-order concerns. (But do little to address the estate planning or transfer of authority from the deceased to designated persons.)

The US Senate is working on the “NO FAKES” act, which seeks to ban recreation of the voice and visual likeness from unauthorized recreation.<sup>47</sup> The bill was reintroduced in April of 2025, with broader support from Google, SAG-AFTRA, major record labels, and OpenAI.<sup>48</sup>

---

<sup>45</sup> Drew Harwell, “Jim Acosta sparks fury with ‘interview’ of dead Parkland teen’s AI avatar,” *The Washington Post*, August 5, 2025, <https://www.washingtonpost.com/technology/2025/08/05/jim-acosta-joaquin-oliver-parkland-ai/>.

<sup>46</sup> “EU AI Act: First Regulation on Artificial Intelligence | Topics | European Parliament,” Topics | European Parliament, August 6, 2023, <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.

<sup>47</sup> NO FAKES Act of 2025, S. 1367, 119th Congress (2025-2026).

<sup>48</sup> Samuel Cohen, “Congress Reintroduces the NO FAKES Act With Broader Industry Support,” *The National Law Review*, April 14, 2025, <https://natlawreview.com/article/congress-reintroduces-no-fakes-act-broader-industry-support>.

The proposed law, however, is just that: proposed. Recent revisions are drawing criticism from privacy-advocacy groups like the EFF, which sees it as a tool for censorship and threatening anonymous dissent.<sup>49</sup>

While legislation seeks to find its footing to deal with this new threat model, the harms involved are obvious: if the deceased was well-known, then their likeness may be recreated for pure profit reasons. If, as in the court cases cited above, the deceased are part of significant legal or cultural events, they may be exploited for emotional impact in court cases. Even those not particularly well-known or significant in other ways may still be targets of general identity theft, especially as the notification system for end-of-life is fragmented and flawed across various jurisdictions.

## 8 Policy and Standards Recommendations

Digital estate planning will only mature if policy, standards, and implementation move in tandem. The risks outlined in Section 3 illustrate how delegation, when poorly designed, can enable exploitation, coercion, and erasure. To counter those risks, the roadmap below outlines how lawmakers, standards communities, and implementers can create systems that protect autonomy while remaining practical at scale. Equally important, these steps must account for cultural diversity, as what constitutes autonomy, consent, or proper succession varies across societies. Without that nuance, even well-designed protocols may fail in practice.

### 8.1 Policy Priorities for Legislators and Regulators

Lawmakers hold the authority to recognize digital assets as a distinct category of property and to protect individuals from abuse after death. Without explicit legal recognition, digital estates remain vulnerable to ad hoc terms of service and inconsistent judicial interpretations. By defining digital assets, extending probate laws, and establishing rights for delegation, privacy, and auditability, policymakers can provide the legal scaffolding that individuals and families need. These priorities also reflect the need for safeguards against coerced or abusive delegation and for mechanisms that operate across jurisdictions, given the global reach of digital platforms.

This starts with formally defining digital assets—including social media, cloud accounts, crypto wallets, and metadata profiles—and extending probate and estate laws to cover them. Policies should also protect individuals from coercion, abuse, and default rules that override their intent.

Key priorities include:

---

<sup>49</sup> Katharine Trendacosta and Corynne McSherry, “The NO FAKES Act Has Changed – and It’s so Much Worse,” Electronic Frontier Foundation, June 26, 2025, <https://www.eff.org/deeplinks/2025/06/no-fakes-act-has-changed-and-its-so-much-worse>.

- **Recognize digital assets in law:** Define digital property explicitly and extend inheritance and probate statutes to cover them.
- **Establish a Digital Estate Bill of Rights**, ensuring:
  - The right to designate digital delegates.
  - The right to revoke delegation before death or incapacitation.
  - The right to privacy and dignity in post-mortem data handling.
  - The right to audit who accessed one's digital identity after death or incapacity.
- **Guard against abuse and coercion:** Require audit trails for delegated access, prohibit automatic authority based solely on kinship, and mandate transparency of consent. Such safeguards must acknowledge that in many societies, family members will expect access as a matter of cultural norm, making it difficult to draw the line between legitimate expectation and coercion.
- **Harmonize jurisdictional approaches:** Promote regional treaties and international guidance so that cross-border platforms cannot sidestep national protections. This will require sensitivity to cultural practices around ancestor veneration, memorialization, and data inheritance, rather than assuming Western legal models are universally applicable.

## 8.2 Recommendations for Standards Bodies

Technical standards, ideally, make policy enforceable. Without interoperable delegation protocols, fiduciaries will continue to rely on insecure workarounds, such as password sharing. Standards communities need to define the vocabulary, data models, and protocols that enable delegation to function reliably across platforms, while embedding privacy and abuse resistance into the design.

Standards bodies should:

- **Define interoperable delegation protocols:** Replace impersonation with true on-behalf-of delegation that preserves the identity boundary between principal and agent.
- **Incorporate core safeguards:**
  - Auditable logs of all delegated actions.
  - Revocation mechanisms that are enforceable even across jurisdictions.
  - Multi-party delegation models to reflect real caregiving and fiduciary networks.
  - Delayed or conditional triggers that activate only after verified death or incapacitation.
- **Develop trust frameworks** to govern identity proofing, death certificate validation, and issuance of digital fiduciary credentials. These frameworks should also consider cultural validation methods—such as religious death rites or communal declarations—that carry social legitimacy even if they lack formal documentation.

- **Pilot cross-industry testing** for conformance, interoperability, and security validation, ensuring real-world usability.
- **Continue the development of delegation semantics** within standards organizations such as the OpenID Foundation, the World Wide Web Consortium, the Internet Engineering Task Force, and the Kantara Initiative, ensuring consistency across identity ecosystems. Coordination should include non-Western stakeholders to ensure that standards reflect diverse legal and cultural practices.

## 8.3 Implementation Pathways and Cross-Sector Collaboration

Even with strong laws and technical standards, adoption will fail without practical pathways for implementation. Governments can embed estate triggers into civil registries and create APIs that notify service providers of death or incapacitation. Platforms can integrate standard interfaces for account delegation, reducing their legal risk and support burden. Civil society can normalize planning through education, templates, and advocacy. And cross-industry pilots can test usability and interoperability before deployment at scale. Collaboration across sectors ensures that digital estate management works for individuals, families, fiduciaries, and platforms alike.

Strong laws and technical standards mean little without credible adoption strategies. Implementation requires coordination across governments, industry, and civil society, with pilot programs to validate usability and resilience. This process will succeed only if it reflects how different cultures already handle legacy, remembrance, and posthumous rights.

Practical pathways include:

- **Government roles:**
  - Integrate estate triggers into civil registries, offering secure APIs for proof of death or incapacity.
  - Support multi-source verification where civil registration is weak or contested. In such contexts, governments may need to rely on hybrid models that include religious authorities, community leaders, or other culturally recognized certifiers.
- **Platform responsibilities:**
  - Implement standard interfaces for account delegation and estate credentials.
  - Phase out proprietary legacy tools that lock families into uneven policies.
  - Offer clear user options for delayed deletion, memorialization, or asset transfer. These options should be adaptable to cultural expectations—for example, perpetual preservation for ancestor veneration or timed deletion for traditions that emphasize impermanence.
- **Civil society and legal networks:**
  - Run public awareness campaigns and digital legacy workshops.

- Provide estate templates and model clauses adapted to cultural and legal diversity.
- Advocate for the rights of minors, marginalized communities, and those in coercive environments.
- **Cross-industry pilots:**
  - Test usability of delegation protocols with diverse populations and edge cases.
  - Validate privacy safeguards and abuse-resistant features in real deployments.
  - Feed pilot results back into standards and regulatory refinements. Pilots should be global in scope, ensuring that solutions are not optimized only for North American or European conditions.

## 9 Conclusion

Death in the digital age is not a tidy matter. The systems we have built for identity and communication outlive us, and in doing so, they challenge long-standing assumptions about autonomy, legacy, and remembrance. A digital estate is not simply the sum of accounts and passwords; it is a contested space where culture, law, technology, and family expectation intersect. Left unmanaged, that space can become a site of exploitation, erasure, or endless conflict. Managed well, it can offer continuity, dignity, and new forms of memory.

This paper has shown that delegation sits at the heart of the problem. Whether through elder abuse, domestic coercion, institutional overreach, or default inheritance rules, poorly designed delegation mechanisms can strip individuals of control in life and distort their wishes after death. Yet delegation is also essential: no estate can be managed without someone empowered to act. The challenge is not whether delegation should exist, but how it should be bounded, supervised, and made accountable.

Cultural and legal traditions offer both caution and guidance. In collectivist societies, family or community expectations shape how authority is exercised; in individualist systems, the emphasis on personal autonomy can clash with the needs of grieving families. Probate law, inheritance customs, and religious rites all offer insights into how societies strike a balance between the rights of the living and respect for the dead. If digital estate planning ignores those traditions, it risks imposing technical solutions that feel alien and illegitimate. The most durable policies and protocols will be those that adapt to cultural variation rather than erase it.

Policy and standards development must now move forward on parallel tracks. Legislators need to clarify the status of digital assets and extend estate protections into the online sphere, while standards bodies must create interoperable protocols for delegation, consent, revocation, and auditability. Neither group can succeed alone. Policy without enforceable technical mechanisms will remain symbolic; protocols without legal force will

remain optional. Implementation, in turn, requires participation by platforms, governments, and civil society to ensure that protections are more than theoretical.

The way forward is not to search for a perfect solution, but to establish principles and practices that reduce harm and respect intent. Common language for roles and responsibilities, auditable delegation protocols, trust frameworks for fiduciary credentials, and cross-industry pilots all form part of the solution. But beyond the technical checklists lies a deeper imperative: to recognize that digital identity is inextricably linked to human identity, and that how we treat digital legacies reflects what we value in the living world.

We are at the beginning of this work, not the end. If stakeholders treat digital estate planning only as a compliance exercise, the result will be uneven protections, cultural dissonance, and systems that entrench abuse. If, however, the identity community treats it as an opportunity—to design for dignity, to balance autonomy with interdependence, and to extend ethical care into the digital sphere—then we can create a foundation that future generations will trust.

In short, the task before us is not just technical. It is cultural, legal, and ethical. The digital identities we leave behind will speak for us long after we are gone. Whether they speak truthfully and respectfully depends on the choices we make now.

# 10 Appendices

## 10.1 Bibliography

American Bar Association. "OpenAI's use of Scarlett Johansson-like voice in ChatGPT exposed gaps in the law," November 21, 2024. Accessed December 17, 2025. [https://www.americanbar.org/advocacy/governmental\\_legislative\\_work/publications/washingtonletter/november-24-wl/openai-scarlett-johansson-1124wl/](https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/november-24-wl/openai-scarlett-johansson-1124wl/).

American College of Trust and Estate Counsel. "The Importance of Cultural Competence in Estate Planning." October 4, 2023. <https://www.actec.org/resource-center/video/the-importance-of-cultural-competence-in-estate-planning/>.

Aries, Philippe. *Western Attitudes Toward Death from the Middle Ages to the Present*. Baltimore: Johns Hopkins Press, 1974.

Banta, Natalie M. "Minors and Digital Asset Succession." *Iowa Law Review* 104 (2019): 1699. <https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2022-10/Minors%20and%20Digital%20Asset%20Succession.pdf>.

Beyer, Gerry W., and Kerri Nipp. "Estate Planning for Cyber Property, Electronic Communications, Cryptocurrency, Non-Fungible Tokens, and the Metaverse." *Estate Planning & Community Property Law Journal* 16, no. 1 (2023). <https://epj.us/volume-16>.

Bloch, Maurice, and Jonathan Parry, eds. *Death and the Regeneration of Life*. Cambridge: Cambridge University Press, 1982.

Buragohain, D., Y. Meng, C. Deng, et al. "Digitalizing Cultural Heritage through Metaverse Applications: Challenges, Opportunities, and Strategies." *Heritage Science* 12 (2024): 295. <https://doi.org/10.1186/s40494-024-01403-1>.

Cherry, Kendra, MEd. "Understanding Collectivist Cultures." *Verywell Mind*, August 5, 2024. <https://www.verywellmind.com/what-are-collectivistic-cultures-2794962>.

Clarke, Ian. "Ancestor Worship and Identity: Ritual, Interpretation, and Social Normalization in the Malaysian Chinese Community." *Sojourn: Journal of Social Issues in Southeast Asia* 15, no. 2 (2000): 273–95. <http://www.jstor.org/stable/41057042>.

"Cloud Contracts - Cloud Legal Project." n.d. Accessed August 21, 2025. <https://www.qmul.ac.uk/cloudlegal/research/cloud-legal-project-papers/cloud-contracts/>.

Cohen, Greyson. "Digital Purgatory and the Rights of the Dead: Protecting Against Digital Disinterment in the Age of Artificial Intelligence." *Cardozo Law Review De Novo* 121 (2023). <https://ssrn.com/abstract=4620092>.

Cohen, Samuel. "Congress Reintroduces the NO FAKES Act with Broader Industry Support." *National Law Review* XV, no. 232 (2025). <https://natlawreview.com/article/congress-reintroduces-no-fakes-act-broader-industry-support>.

Davis, Richard H. "Cremation and Liberation: The Revision of a Hindu Ritual." *History of Religions* 28, no. 1 (1988): 37–53. <http://www.jstor.org/stable/1062167>.

Desert Law Group. "Incorporating Cultural Beliefs into Your Estate Planning." October 17, 2024. <https://desertlawgroup.com/blog/cultural-beliefs/incorporating-cultural-beliefs-into-your-estate-planning/>.

Dominus, Susan. "A.I. Avatars and the Brave New Frontier of Life After Death." *New York Times*, June 17, 2025. <https://www.nytimes.com/interactive/2025/06/13/magazine/ai-avatar-life-death.html>.

Fagone, Jason. "The Jessica Simulation: Love and Loss in the Age of A.I." *San Francisco Chronicle*, July 23, 2021. <https://www.sfchronicle.com/projects/2021/jessica-simulation-artificial-intelligence/>.

Feifel, Herman. *The Meaning of Death*. McGraw-Hill Companies, 1959.

Graeber, David. "Dancing with Corpses Reconsidered: An Interpretation of 'Famadihana' (In Arivonimamo, Madagascar)." *American Ethnologist* 22, no. 2 (1995): 258–78. <http://www.jstor.org/stable/646702>.

———. "Painful Memories." *Journal of Religion in Africa* 27, no. 4 (1997): 374–400. <https://doi.org/10.2307/1581909>.

HereAfter AI. Accessed August 20, 2025. <https://www.hereafter.ai/>.

Hood, Ralph W., and Ronald J. Morris. "Toward a Theory of Death Transcendence." *Journal for the Scientific Study of Religion* 22, no. 4 (1983): 353–65. <https://doi.org/10.2307/1385773>.

Jain, Dipika. "Regulation of Digital Healthcare in India: Ethical and Legal Challenges." *Healthcare* 11, no. 6 (March 21, 2023): 911. <https://doi.org/10.3390/healthcare11060911>.

Jones, M., Nadalin, A., Campbell, B., Ed., Bradley, J., and C. Mortimore, "OAuth 2.0 Token Exchange", RFC 8693, DOI 10.17487/RFC8693, January 2020, <<https://www.rfc-editor.org/info/rfc8693>>.

Kantara Initiative. "User-Managed Access: Taking Control of Your Data Sharing | Kantara Initiative," May 9, 2025. <https://kantarainitiative.org/work-groups/uma/>.

Kim, Juliana. "Family Shows AI Video of Slain Victim as an Impact Statement — Possibly a Legal First." *NPR*, May 12, 2025. <https://www.npr.org/2025/05/07/g-s1-64640/ai-impact-statement-murder-victim>.

Klee, Miles. "How Celebrities Are Fighting AI Deepfakes of Themselves." *Rolling Stone*, January 27, 2025. <https://www.rollingstone.com/culture/culture-features/ai-deepfakes-celebrities-1235246116/>.

Lifton, Robert Jay. *The Broken Connection: On Death and the Continuity of Life*. New York: Simon and Schuster, 1979.

Luka, Inc. *Replika*. Accessed August 20, 2025. <https://replika.com/>.

Magege, Rachel, and Bonaventure Saturday. "Mine Is Yours - Pollicy." *Pollicy*, April 30, 2025. <https://pollicy.org/resource/mine-is-yours/>.

Mandelbaum, David G. "Social Uses of Funeral Rites." 1965.

McSherry, Katharine Trendacosta, and Corynne McSherry. "The NO FAKES Act Has Changed — and It's So Much Worse." *Electronic Frontier Foundation*, June 26, 2025. <https://www.eff.org/deeplinks/2025/06/no-fakes-act-has-changed-and-its-so-much-worse>.

MOSIP. "MOSIP." Accessed December 17, 2025. <https://www.mosip.io/>.

OpenID Foundation. "eKYC & IDA Working Group - OpenID Foundation." OpenID Foundation - Helping People Assert Their Identity Wherever They Choose, January 23, 2025. <https://openid.net/wg/ekyc-ida/>.

Opler, Marvin E. "An Interpretation of Ambivalence of Two American Indian Tribes." *Journal of Social Psychology* 7 (1936): 82–116.

Palgi, Phyllis, and Henry Abramovitch. "Death: A Cross-Cultural Perspective." *Annual Review of Anthropology* 13, no. 1 (October 1, 1984): 385–417. <https://doi.org/10.1146/annurev.an.13.100184.002125>.

Parsons, Elsie Clews. *Pueblo Indian Religion*. 2 vols. Chicago: University of Chicago Press, 1939.

Perez, Sarah. "YouTube Now Lets You Request Removal of AI-generated Content That Simulates Your Face or Voice." *TechCrunch*, July 1, 2024.

<https://techcrunch.com/2024/07/01/youtube-now-lets-you-request-removal-of-ai-generated-content-that-simulates-your-face-or-voice/>.

———. "YouTube Expands Its 'Likeness' Detection Technology, Which Detects AI Fakes, to a Handful of Top Creators." *TechCrunch*, April 9, 2025.

<https://techcrunch.com/2025/04/09/youtube-expands-its-likeness-detection-technology-which-detects-ai-fakes-to-a-handful-of-top-creators/>.

Peters, Jay. "Meta Moves on from Its Celebrity Lookalike AI Chatbots." *The Verge*, July 30, 2024. <https://www.theverge.com/2024/7/30/24209918/meta-celebrity-lookalike-ai-chatbots-moves-on>.

Rahman-Jones, Imran. "Pornographic Taylor Swift Deepfakes Generated by Musk's Grok AI." *BBC*, August 8, 2025. <https://www.bbc.com/news/articles/cwye62e1ndjo>.

Rao, Ramesh N. "Talking to the Dying: Hindu Views, Hindu Ways." *International Journal of Sociology of the Family* 36, no. 1 (2010): 65–76. <http://www.jstor.org/stable/23070779>.

Sharwood, Simon. "Put Your Usernames and Passwords in Your Will, Advises Japan's Government." *The Register*, November 21, 2024. [https://www.theregister.com/2024/11/21/japan\\_digital\\_end\\_of\\_life/](https://www.theregister.com/2024/11/21/japan_digital_end_of_life/).

Singleton, Amanda. "Prepare a Digital Estate Plan for Future Caregivers." AARP, June 2, 2025. <https://www.aarp.org/caregiving/financial-legal/digital-assets-planning/>.

Singleton, Tom. "Tom Hanks Warns Dental Plan Ad Image Is AI Fake." *BBC*, October 2, 2023. <https://www.bbc.com/news/technology-66983194>.

Society of Trust and Estate Practitioners. "Protect Your Digital Memories Campaign Toolkit." Accessed August 20, 2025. <https://www.step.org/digital-assets/protect-your-digital-memories-campaign-toolkit>.

Solender, Andrew. "Dead congressman promotes candidate for his seat on social media." *Axios*, June 24, 2025. Accessed December 17, 2025. <https://www.axios.com/2025/06/24/gerry-connelly-james-walkinshaw-dead-social-media>.

Sovrin Foundation. "Guardianship." May 28, 2023. <https://sovrin.org/guardianship/>.

Stamp, Niall. 2024. "GDPR and Personal Data After Death - GDPR EU." GDPR EU. October 25, 2024. <https://www.gdpreu.org/gdpr-faqs/gdpr-and-personal-data-after-death/>.

StoryFile. "Authentic Interactions." Accessed August 20, 2025. <https://www.storyfile.com/>.

TechTello. "Learn and Be Better Everyday — TechTello." September 3, 2024.  
<https://www.techtello.com/>.

Transnational Management Associates Limited (TMA World). "Country Navigator | The No. 1 Cultural Intelligence Training Platform." May 20, 2024.  
<https://www.countrynavigator.com/>.

McSherry, Katharine Trendacosta and Corynne. "The NO FAKES Act Has Changed – and It's so Much Worse." Electronic Frontier Foundation, June 26, 2025.  
<https://www.eff.org/deeplinks/2025/06/no-fakes-act-has-changed-and-its-so-much-worse>.

Tsuji, Yohko. "Rites of Passage to Death and Afterlife in Japan." *Generations: Journal of the American Society on Aging* 35, no. 3 (2011): 28–33. <https://www.jstor.org/stable/26555791>.

Uniform Law Commission. "Fiduciary Access to Digital Assets Act, Revised," 2015. Accessed December 17, 2025. <https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22>.

Harwell, Drew. "Jim Acosta sparks fury with 'interview' of dead Parkland teen's AI avatar." The Washington Post, August 5, 2025.  
<https://www.washingtonpost.com/technology/2025/08/05/jim-acosta-joaquin-oliver-parkland-ai/>.

Wulf, Andrea. *Magnificent Rebels: The First Romantics and the Invention of the Self*. New York: Alfred A. Knopf, 2022.