International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2025 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Digital Afterlife: Who owns your Social Media Data after Death?

Srishti Keshri[a]

[a]Amity University, Jharkhand, India

Received 08 November 2025; Accepted 08 December 2025; Published 12 December 2025

The concept of a digital afterlife has emerged as a significant legal and ethical challenge in the twenty-first century, as individuals increasingly leave behind vast amounts of personal, financial, and creative data stored online. This article examines the question of ownership and control of social media accounts and digital assets after death, analysing whether such data should be treated as inheritable property or protected personal information. It explores the legal ambiguity surrounding posthumous data rights, highlighting the conflict between platform terms of service, privacy obligations, inheritance laws, and the emotional needs of families. Through a comparative analysis of international frameworks, including those of the United States, the European Union, the United Kingdom, and India, the paper identifies the absence of a uniform legal approach, particularly in the Indian context. It also addresses ethical concerns, including posthumous privacy, data monetisation, digital grief, and identity misuse. The article argues for clearer legislation, transparent platform policies, and greater user awareness through digital wills to ensure dignity, accountability, and fairness in managing digital legacies after death.

Keywords: *social media, digital afterlife, ownernship.*

INTRODUCTION

Human life in the twenty-first century has grown into a vast digital world wherein people create, share, and store information at every second of their lives. Every photo uploaded on Instagram, every tweet tweeted, every video published on YouTube, and every message saved form part of one's digital existence. The digital life goes on and on long after the person who created it dies, forming what at this point has come to be known as the digital afterlife. The key question then arises: Who shall be considered as the owner of that data once the creator is dead?

The notion of digital afterlife became important, as every year millions die while leaving large footprints in cyberspace; this includes emails, cloud storage, social media posts, and digital wallets, among other online records. The challenge is that the laws across countries remain unclear. In fact, most countries still don't have legislation to determine whether data should be treated as property that can be inherited, or personal information that is entitled to protection even after death.

Technology companies filled this legal gap with their own policies. On platforms like Facebook, users can name a "legacy contact" to manage a memorialised account. Google has the "Inactive Account Manager," which allows users to decide what happens to data after a period of inactivity. Instagram and Twitter permit family members to request an account's removal, but limit access to private data. None of these policies fully or consistently settles the ownership questions, especially in cases in which emotional and legal interests' conflict. Accessing the accounts of loved ones, whether for financial or sentimental reasons, is often a challenge that families face. However, in many jurisdictions, privacy rights extend long after an individual has died, and whether it is right to place the privacy of the dead above the needs of their family is a major ethical question. Another issue involves cross-border data storage: a person may live in one country, use a platform based in another, and have data stored across multiple nations. This also makes digital inheritance a lot more complex. Moreover, digital platforms consider user data as part of the assets of their business. They have legal control over the servers, but data has a personal nature, making the very question of ownership quite fuzzy. In the absence of clear-cut rules, there is much uncertainty for families, companies, and even governments. These challenges in this direction create an increasing demand for comprehensive digital legacy laws, education of users, and standardised platform policies. The idea here is to encourage individuals

to prepare their digital afterlife by using such legacy tools, preparing digital wills, and making family members aware of where online accounts are maintained. The digital afterlife really creates a modern question of identity, privacy, and ownership. Technology has moved very fast, but the law and its ethics have not; thus, society has to consider carefully what really happens with our online selves following our death.

UNDERSTANDING DIGITAL AFTERLIFE

Meaning of Digital Afterlife: The digital afterlife is the state, management, and control of the online data of a person after death. Much electronic information is generated, even unwittingly, about what will happen in the long run. This ranges from the use of social media commentary to financial documents stored on servers that outlive the individual. Thus, the digital afterlife contemplates what happens to these digital assets and who has the authority to access, preserve, or delete them.

Apart from personal memories, a number of digital assets have economic relevance, too. Online bank accounts, digital payment services, and cryptocurrency wallets actually store real money that might be inheritable. In contrast, subscription accounts on platforms like Netflix, Amazon, or Spotify do not hold financial value; again, proper closure or transfer requires attention. Messaging platforms like WhatsApp and Telegram store highly private conversations; questions arise whether family members should have access to them or whether privacy should be kept even after death.

Digital afterlife also refers to all the digital creations that a person leaves behind: blogs, diaries, comments, posts, YouTube videos, and digital artworks. These may continue to inspire people or to earn money. Because these assets are stored on the servers owned by private companies, users do not fully “own” them in the traditional sense, but are bound to the terms-of-service agreements that often limit access after death.

Importantly, digital data does not automatically disappear with the death of the owner. Quite the contrary, platforms keep the data according to their policies, and these policies are often totally different from one platform to another. Some allow one's family to request deletion, while others offer other services, which may include memorialization or account transfer. In some

cases, national laws may override the policies of those platforms, especially in concerns related to inheritance or privacy.

Components of Digital Assets: Not all of the digital assets one leaves upon death are created equal. They vary for many reasons in purpose, value, and level of privacy, and they even vary with respect to how the law treats them. Distinguishing these kinds of assets provides a framework for understanding who might have any rights of access, inheritance, or management of the assets of the user who has died.

Each Category raises a different Set of Legal, Ethical, and Emotional questions - to be discussed below –

Communication Data: Communicative data involves emails, private messages, chats, posts, comments, and interaction histories. Such kinds of data are deeply personal in that most of them are intimate conversations, confidential exchanges, and sensitive emotional content. They thus also have strong privacy implications continuing beyond death in many jurisdictions. This category is most debated because it directly touches upon personal autonomy and posthumous privacy.

Creative Data: Creative data are digital works that a user has created, including but not limited to videos, manuscripts, photos, music compositions, designs, blogs, e-books, and other digital art. They may have value in copyright terms-that is to say, they can be passed on, like more traditional intellectual property, to the beneficiaries upon the death of the creator. Royalties can be legally distributed to any heirs, publication rights managed, or rights to distribute the digital content exercised. Thus, creative data is economically transferable, has legal value, and falls within copyright jurisdictions often for 50-70 years after a person's death.

Financial Digital Assets: Examples include cryptocurrency wallets, online banking accounts, PayPal balance, trading accounts, digital gold, and online investment platforms. These assets have their intrinsic monetary value and hence are granted the status of being inheritable by financial and inheritance laws. However, access might be very difficult because of encryption, a password, or two-factor authentication. In the context of cryptocurrency, the loss of private keys can mean permanent loss. Thus, financial digital assets require a lot of planning and documentation so that their retrieval by legal heirs is possible.

Identity-Based Data: Identity-linked data includes usernames, profile pictures, biometric recordings, voice notes, and personal information that, in essence, is integrally linked with the identity of a certain individual. These assets cannot be inherited because they are closely tied to the deceased's personal identity. Platforms generally lock this type of data under privacy rules, forbidding others from impersonating or misusing it.

Behavioural Data: It includes search history, browsing patterns, location logs, purchase preferences, and algorithmic profiles created by companies. It has immense value to corporations for advertising and analytics, but very rarely carries personal or inheritable value; ownership largely stays with the company, not with the user. The categories make it quite clear which digital assets are transferable, which should remain private, and who may have legitimate rights over them upon death.

WHY DIGITAL AFTERLIFE MATTERS TODAY?

The billions of digital footprints that remain after one's death in this modern world include photos, conversations, e-mails, comments, memories, and personal files stored on various platforms. Thereby, the question of digital afterlife gains importance that touches on aspects such as technology, law, ethics, emotions, and human dignity.

Access to a loved one’s digital information is an essential part of the family’s grieving process. The final messages and photos saved, the posts allowing the family emotional closure, let the family remember and understand the unfinished conversations and keep memories of the beloved who is now gone. Actually, access is not always provided because most of these platforms restrict entry for privacy protection purposes.

Only nowadays do the legal systems begin to recognise that inheritance today is not solely about physical property. Digital property can range from cryptocurrency and online accounts to monetised YouTube channels; it may have very real economic value. Now, the law must address things like digital wills, ownership rights, the transferring of data upon death, and permissions for access.

At the same time, if these accounts are not disabled, they offer a host of potential hazards. Criminal misuse for committing hacking, fraud, impersonation, or sending spam from a deceased person's account is also becoming common. These facts place greater responsibilities

on companies for the security of accounts and the protection of user data when the user is no longer alive.

Another serious issue is identity theft. Usually, the accounts that hackers attack are those that have remained inactive, since those are not looked after. Misusing a dead person's identity may cause emotional harm to families and even bring legal complications.

Despite these challenges, there is value in some aspects of digital afterlife: firstly, personal documents, videos, and creative works record a rich history to family and future generations since they record history in ways that physical items cannot. The issue of digital afterlife involves, therefore, a matter not of purely technical concern but one touching deeply on legal rights, ethical principles, family relationships, and respect owed to persons even after death.

LEGAL DIMENSIONS OF OWNERSHIP AFTER DEATH

Do Users Own Their Data? Most people think that on social media, the photos, posts, comments, or videos uploaded by them are fully "theirs." While that may be partially true, the full legal picture is a lot more complex than it seems. Ownership and control are two different things in the digital world, where this distinction becomes critical after a user's death.

Legally speaking, by uploading any original content, such as photos, blogs, videos, and artwork, you still retain copyright ownership. That is to say, even after you die, you are still the maker and the legal owner of the intellectual property. Copyright law protects your creative work for decades, and usually passes your creations to your legal heirs.

But the moment you sign up on social media, you agree to its Terms of Service. These long contracts, rarely read by users, provide the service with a blanket license to store, use, distribute, and manage your content. They grant businesses the capabilities and permissions to allow account access, change privacy settings, enable deleting one's account, or handle user data in general.

It is the first case of its kind where –

- You own the content, such as a photo.
- But the platform owns the account in which the photo is stored.

While the digital content is yours, the platform controls the space in which it exists. In that regard, the platform also controls what will happen with your account when you die-whether it will be memorialised, deleted, or frozen.

This leads to serious complications when families seek to access the data of a deceased person: parents may want to read their child's final messages, spouses may need important files or memories, but a platform can deny access, despite emotional and occasionally legal claims to the contrary, since ToS protects the privacy of users even after death.

While technically, users “own” their content, the control remains with the platform, and the whole concept is very confusing, with a lot of legal ambiguity regarding digital assets at death.

WHAT HAPPENS WHEN A USER DIES?

When a social media user dies, that digital presence does not just vanish into thin air. Instead, one of three possible eventualities usually occurs: the platform keeps the data, the data is deleted, or the family attempts to access it. But who has the final say over this digital legacy? That's significantly more complicated. Four main factors typically clash with one another: platform policies, national laws, the desires of the deceased person, and the needs of the family on an emotional level.

Policies of the Platform: Each of these has its own policies regarding what happens to an account upon the death of a user, whether an account can be memorialised, deleted upon request, or, in very few cases, private messages accessed. Because users have agreed to the terms of service upon sign-up, companies can often claim the most significant authority. Most systems afford greater importance to privacy than inheritability, even in the case of immediate family members.

National Laws: The legal perspective of digital inheritance is different in different countries. Digital content, which some nations see as property to be inherited, others take as a form of private information that should remain protected even after the owner has died. In some jurisdictions, courts have ordered the surrender of certain data from platforms to families, while in other countries, this same company is legally bound to refuse the request. This inconsistency creates confusion and often leads to legal disputes.

Instructions of Deceased Increasingly: It is possible to indicate preferences for after one's death with services like Google's Inactive Account Manager or Facebook's Legacy Contact. When such instructions exist, they generally take precedence over other claims. A clearly written digital will can also affect how data should be treated.

Family's Emotional Needs: Access is often sought by families for closure, sentiment, or to regain memories that are important to them. Emotional needs seldom carry legal weight unless supported by national laws or user instructions. Because these four forces often clash, different jurisdictions reach different conclusions, and no clear rule can be established. Determining "who has the final say" thus becomes one of the most debated topics in the realm of digital afterlife law.

Two Legal Theories of Digital Inheritance –

Explanations of digital inheritance generally consider two major theories, namely, the Property-Based Approach and the Privacy-Based Approach. Both are applied today by most countries, either singly or in combination, depending upon the kind of digital asset.

Property-Based Approach: This theory treats digital assets much like physical property: money, jewellery, land, documents, etc. Digital property may be legally inherited in case the asset itself carries some economic and financial value. Examples of this could include a cryptocurrency wallet, an online bank account, e-commerce stores, monetised YouTube channels, and manuscripts in digital form. Since these are revenue-generating assets representative of actual wealth, they are considered to be passed on to the legal heirs through the medium of a will or through the laws of succession. It therefore gives emphasis to the economic dimension of the digital property.

Privacy-Based Approach: The more sensible approach that a privacy-based theory takes toward the treatment of digital accounts is to regard them as a part of the individual self, somewhat like a diary or private letters. Thus, emails, WhatsApp messages, private chats, direct messages on social media, photos stored, and search history-all are very personal areas. In that respect, since usually privacy rights survive even death, these assets, in that sense, are inalienable to heirs. This is the approach taken when platforms try to deny access even to close family members.

Contractual Rights v Inheritance Rights: The main tension within the area of digital afterlife law involves the pull between contractual rights and inheritance rights. Every time a user creates a social media account, they enter into a legally binding contract known as the Terms of Service. These agreements detail what the technological platform will store, manage, and protect with respect to the user's data. More importantly, they detail what happens with an account after its owner dies. Because users accept these terms, knowingly or unknowingly platform gains strong legal authority over the digital account.

This is in contrast to the more traditional concept of inheritance, where legal heirs have rights to access or inherit the possessions of the deceased. Digital accounts are usually assumed to fall under this category of possessions by families; however, most platforms consider their accounts as licensed services and not property to be inherited. This means access to the account is curtailed upon the death of such a user and cannot be transferred to heirs, as physical assets would.

A well-known example illustrates this conflict:

Whereas a father could legally inherit his deceased daughter's physical belongings, the same legal authority fails to grant him access automatically to her messages on Facebook. Facebook's ToS favours user privacy-even after death-and precludes anyone from entering into the account or reading private conversations. In that case, platform contractual duties override family inheritance rights.

This is an example of great legal tension: on the one hand, families might need access to gain closure or retrieve key files or understand different circumstances surrounding death; on the other hand, platforms should not breach user privacy and national data protection laws. Courts in the world have grappled to harmonise these competing rights. Therefore, the contradiction between the ToS contract and the inheritance law remains one of the greatest hindrances to digital afterlife governance. It points to the need for clearer laws on digital legacy and more transparent platform policies.

Jurisdictional Problems: One of the biggest challenges with regard to digital afterlife law involves issues of jurisdiction. There is no single geographical space where digital data remains present. A user may be living in India while using a social media platform headquartered in

California or Ireland, and their data may be stored on cloud servers in the United States, Europe, or even multiple countries at once. The multi-layered configuration creates serious legal confusion.

The central question becomes: Whose law applies?

- Should it be Indian inheritance laws, for the deceased user lived and died in India?
- Should it be the U.S. privacy laws because the data is on American servers?
- Or should it be European Union laws, since the company has headquarters in Ireland, abiding by GDPR rules?
- Or do platform policies override all national laws?

There is no comprehensive international framework for digital inheritance or posthumous data rights. Countries have their own legislation on data protection, privacy regulations, and succession rules, most of which stand in direct conflict with others. The consequences are that bereaved families may face complicated, lengthy, and very often unsuccessful attempts to gain access to digital accounts because digital footprints cross borders so easily, and the question of ownership becomes even harder to resolve. This lack of global uniformity makes the digital afterlife one of the most challenging legal issues of the modern era.

INTERNATIONAL LEGAL FRAMEWORKS

United States: RUFADAA: Among all countries, only the United States has gone to the extent of adopting one of the most structured legal approaches toward digital inheritance through RUFADAA. Most states in the U.S. have adopted RUFADAA in their effort to try to mediate the growing number of disputes between families, digital platforms, and privacy laws upon the death of a user.[1] Its main purpose remains to decide how the digital assets are to be accessed, transferred, or protected upon the death or incapacitation of an individual.

Most importantly, RUFADAA legally acknowledges digital assets as property. Included are things like emails, material on social networking sites, documents stored online, photos, and even financial records in digital form. Unlike tangible property, though, access is not necessarily

[1] Sara Azad, 'A Guide to Managing Online Accounts After the Death of a Loved One' (*Willful*) <https://www.willful.co/learn/online-accounts-after-death> accessed 07 November 2025

automatic. In an attempt to balance rights of inheritance against privacy concerns, RUFADAA strikes a careful balance by establishing a tiered structure.

The user's expressed wishes are, nevertheless, the most important factor under the law. Where the user has specified their settings through services like Google's Inactive Account Manager or Facebook's Legacy Contact, for example, such instructions will prevail over all other claims of ownership. This way, the individual may remain in control over his or her digital legacy.

First, RUFADAA seeks respect for platform Terms of Service; even when heirs do request access, platform policies may restrict or deny entry to parts of an account, including private messages. This would avoid forcing platforms to violate privacy obligations.

General inheritance laws would apply only after the user's instructions and platform policies are accounted for. That would allow fiduciary access, especially to any material with financial or administrative relevance: executors, trustees, or court-appointed representatives.

In this respect, RUFADAA will surely protect user privacy, but it will provide a legal avenue for the heirs to get meaningful information. It does not support unlimited private communication access but allows controlled transfer of digital property. In that way, the U.S. model seeks to balance personal autonomy, the emotional needs of families, and the responsibilities of digital platforms.

European Union: GDPR: The European Union’s GDPR is one of the most powerful data protection frameworks in the world, and it says very little about what happens to personal data upon a person's death. Most of the provisions within the GDPR are designed for the rights of living individuals; therefore, post-mortem control is a matter left to individual member states, which leads to divergent national approaches. All this eventually created a patchwork of laws across Europe: some countries emphasise privacy even at death, while others recognise digital assets as part of a person’s estate.

France, for instance, has taken an outright stand on the issue of privacy. While families can request some measures, such as closing accounts or their memorialization, they will not generally be allowed access to the content itself, such as messages or emails, unless the deceased

had expressed authorisation in that respect. In that sense, French law underlines the digital dignity of the dead and respect for the latter's autonomy.

But Germany treats digital assets no differently than tangible possessions. In one landmark ruling, Germany's Federal Court of Justice ruled that the parents of a deceased girl could inherit her Facebook account and messages, much like a diary or letters. It was a decision that leaned heavily on property rights and inheritance laws over platform restrictions on privacy.

Speaking broadly, Europe continues to lean toward the consideration of digital assets as inheritable, but weighs that against the privacy concerns within national legal systems.

United Kingdom: There is no single, uniform law in the UK on digital inheritance, and therefore, a family has to go through a fragmented set of laws. Those digital assets that are based on copyright, such as photos, written works, and other creative content, are treated as property and can be inherited under normal succession laws. Personal digital accounts, on the other hand, people create these for e-mail, social networks, and cloud storage, and are mainly dealt with under each respective service's terms, which generally forbid post-mortem access. This often means that in practice, it is very hard for the family to recover useful data, messages, or photos for emotional closure. Explicit legislation is lacking in this respect; thus, there is uncertainty and reliance on the policies of individual platforms or court intervention may be required.

India: Current Situation: As things stand, there is no clear legal framework on digital inheritance in India, and that leaves a great deal of uncertainty for the families, platforms, and even courts. Though the main legislation that governs electronic data and its online use is the Information Technology Act, 2000, the question as to what happens to the digital assets created by a person after he dies has not been answered. Issues of access to social media accounts, e-mail, cloud data, or digital wallets thus remain unaddressed in statutory law.

While this newly passed Digital Personal Data Protection Act 2023 is a big reform in the field of privacy regulation, it protects the rights of the living only and extends neither privacy nor control over the data of a dead person. Hence, this gap in legislation creates a situation where confusion arises as to whether family members can request, under the law, access to or deletion of the digital content of a dead person. Since no statute so far in the law has defined the ownership of digital assets upon one's death, Indian families are left using internal policies enacted by various

multinational technology companies. Decisions like allowing accounts to be memorialised, deleted, or just restricted usually remain in the discretion of the platforms alone, according to the terms of global service and not under Indian law. This also leaves them emotionally distressed for not being able to access the last photos, messages, or other important documents. Indian courts, too, have not set any important precedent on the question of digital inheritance. Only a few scattered petitions have cropped up, usually for access to email accounts or crypto assets of the deceased. But without guiding statutes, courts tend to fall back on principles of contract law, meaning the Terms of Service signed by the user often override family claims. More than this massive digital population, ever-growing dependence on online assets from social media to fintech hastens the need to clearly define the law of digital inheritance. To begin with, such a law must spell out the ownership, rights of access, powers of the executor, limits of privacy and obligations of digital platforms upon the death of a user. In the absence of clarity, Indian families continue to fight hurdles of legality, emotions, and procedures in the digital afterlife.

Platform-Specific Policies on Digital Afterlife: The question of what happens to their digital life — social media profiles, email, cloud-stored photos, messaging apps and professional accounts — becomes all the more urgent when someone dies.[2] Companies approach this "digital afterlife" in very different ways: some offer memorialization or legacy options that would allow family and friends to keep a presence up, without full access; others permit heirs to request deletion upon proof of death; and a few maintain strict privacy protections, effectively locking the data away. Below, I expand on the major platforms you listed, explain the practical consequences for families and executors, and offer short, practical advice for users who want to plan.

Facebook (Meta): There are two main post-mortem pathways offered by Facebook, which involve memorialization and legacy contacts. Memorialised accounts carry a "Remembering" label; they remain visible to the same audience the deceased used while alive, subject to privacy settings. Friends can see posts and leave tributes, but nobody may log in as the deceased or read private messages. This preserves the person's profile as a place for public grief and remembrance while protecting private communications.

[2] Srishti Sinha, 'DIGITAL AFTERLIFE AND INHERITED DIGITAL ASSETS' (*The Amikus Qriae*) <https://theamikusqriae.com/digital-afterlife-and-inherited-digital-assets/> accessed 07 November 2025

A legacy contact is a person that the account holder picks to manage parts of a memorialised account: changing the profile picture, pinning a post, responding to new friend requests, and requesting account removal. Importantly, the legacy contact cannot log into the account, cannot read private messages, and cannot post as the deceased beyond the features Facebook provides. If no legacy contact has been set, heirs still can request deletion, but they then must provide proof of death and, where appropriate, proof of relationship. The combination of memorialization and limited managerial power tries to balance honouring the deceased with preserving privacy and preventing impersonation.

Instagram: Meta-owned Instagram works along the same lines: accounts can be memorialised or removed upon request with proof of death. Memorialised Instagram accounts display "Remembering" and continue to show posts and images; friends can leave comments. Similar to Facebook, no one can log in as the deceased, and private messages and direct messages remain inaccessible. For families, this means that treasured photos and public interactions can be kept, but private conversations remain private, unless the user has previously shared login/access details with a trusted person.

Google (Gmail, YouTube): Google's Inactive Account Manager, by contrast, is more granular. This allows the user to specify a timeout period of inactivity, six months or a year, after which Google treats the account as inactive. The user can name trusted contacts who will be contacted and can be given access to selected data, or the account can be set up to be deleted automatically. It gives the owner of the account some advanced control to select what to share-emails, photos, Drive files, YouTube content-and with whom.

But if the Inactive Account Manager is not set up, the default for Google is very conservative: it rarely shares account data after death, and then only after legal proof and formal requests. For families, proactive configuration of the Inactive Account Manager is the clearest way to avoid surprises and give access to loved ones to the important documents, photos, or channels.

Twitter (X): Twitter traditionally took a much harder line: the service does not offer a standard process for relatives to take control of the direct messages or account of a deceased loved one. In practice, Twitter will delete an account upon receipt of a request from a relative with proof of death; the company will not disclose the contents of messages. The implication of all this is that

while a public timeline might be disabled or deleted at the request of next-of-kin, private conversations and some account content would remain locked away. The bottom line is that Twitter/X provides very limited accommodation of post-mortem access, prioritising the need to maintain privacy and security over the rights of kin to data.

WhatsApp: WhatsApp does not provide for a legacy or any formal bereavement process. While accounts may be deleted after extended inactivity, WhatsApp's end-to-end encryption means message contents are not stored on company servers in such a way as to be readily accessible. There is also no mechanism for account control to be transferred. In practical terms, this means WhatsApp cannot provide family members with a deceased person's chat history unless they already had the device and backups (e.g., a local phone backup or cloud backup made before death) and the account credentials to restore it. The combination of encryption and the absence of a legacy policy places responsibility on users to make arrangements for access if they wish others to retain their chat history.

LinkedIn: Generally, LinkedIn will accommodate a request from a family member to remove a profile of someone who is deceased. The company absolutely will not grant access to private messages. LinkedIn’s emphasis is on professional identity and reputation; taking an account down upon request helps families preserve the deceased's privacy and avoid unwanted job solicitations or impersonation. For most executors, the process generally involves providing proof of death and making such a request through LinkedIn's support channels.

ETHICAL ISSUES SURROUNDING DIGITAL AFTERLIFE

Privacy after Death: Does the right to privacy vanish at the moment of death? Ethically, most philosophers and scholars of privacy say there is no cutoff. The right to privacy is deeply entangled with personal dignity, autonomy, and the control that one has over their narrative-all things that in some moral sense survive a person's death. Even as most legal protections often lapse or change at that moment, the ethical claim to protect certain intimate aspects of a person's life can remain. Disclosure of private messages, browser history, or health data allows intimate facts about someone to be made public that they would never have agreed to make public; this can, then, be a violation of posthumous dignity.

There are also competing moral claims: for families, access may be desired for closure or to understand the circumstances of the death; rarely, the public interest may demand disclosure, for example, to stop harm or solve a crime. The considered ethical position would treat privacy after death in a context-sensitive way: private communications and sensitive data would be protected unless there was a compelling, proportionate reason to disclose and even then, only to the extent necessary.

Emotional Rights of Family: Family members and close friends have a valid emotional and psychological interest in the digital remains that their loved ones have left behind. Common reasons usually include:

- Retrieving the last photos and videos of sentimental value.
- Reading final messages that may bring comfort or closure.
- Save those memories by backing up, creating scrapbooks, or memorial pages.
- Establishing the circumstances of death when conditions are such that ambiguity or foul play may exist.
- Protect the deceased person against embarrassment, harassment, or fraud by managing their online reputation.

These are emotional rights, ethically entitled to respect. Denials of access to families can heighten grief and leave questions unanswered. However, these do not override the interests of the dead in privacy. The ethical challenge is to develop processes that respect both: allow limited sensitive access if it truly assists grieving or serves a legitimate purpose, but protect those intimate details which a reasonably privacy-conscious deceased would have kept private.

Posthumous Reputation: The reputation of a deceased continues to have moral value. Narratives of impersonation, misrepresentation and adversarial action against the dead have consequences that amount to tangible harm for families and communities. Examples:

- Accounts are getting hacked for distributing misinformation or scamming people.
- The posting of malicious content that affects the person's memory.
- Editing public profiles of the deceased without authorisation to remove or distort the record of their achievement.

The protection of posthumous reputation is an ethical duty binding the platforms, families, and society together. The roles for the platforms are to ensure that abuse is avoided through speedy takedown procedures, memorialization modes, and checks against impersonation. It should be easy for families to report and correct damaging content without giving them free license to rewrite the identity of the dead. Interventions should be transparent and narrowly tailored: removing or correcting content that is false, malicious, or harmful, while preserving those that form part of the historical record or public interest.

Ownership v Identity: Treating social media accounts as pure property completely misses an important distinction: these accounts are entwined with a person's identity. A profile, posts, and networks of followers represent who the person was-socially, politically, and emotionally. Giving complete control to heirs of accounts, as if they were tangible property, opens up several harms: exposing sensitive relationships or secrets the dead had kept private intentionally. Fueling family conflicts over what to keep or delete. Disclose confidential professional or legal communications. Change the voice of the dead in ways that would lie about them. Ethically, principles of inheritance have to be weighed against respect for the person. One possible practical ethical framework could be a presumptive privacy shield: presume private content stays restricted unless the deceased has explicitly authorised access or a compelling reason exists, such as a legal investigation. Where users leave clear instructions, such as through legacy settings or wills which specify their digital wishes, it is generally those directions that should dictate the outcome. Where no instruction is given, neutral third-party oversight can balance competing claims, such as through the courts or appointed digital executors who follow standardised principles.

Data Monetisation after Death: One growing ethical issue could be that companies might continue to analyse, monetise, and extract value from the data of the deceased users in instances such as: Using past behaviour to train AI models. Profiling of deceased users for the improvement of ad-targeting algorithms. Mining personal content for synthetic media or derivative products. Key questions include: Do companies have moral license to profit from a person who cannot consent? Does the gathering of data on deceased users disrespect their personhood? Many would say that monetisation of data posthumously is ethically problematic. Consent is the basis of any valid use of data; after death, the person cannot even withdraw consent or state preferences. Even where legal terms give a broad right to companies, ethics calls for restraint. Companies should not exploit content that was an intimate self-expression. It

would be more ethical to put in place transparent and respectful posthumous data policies that restrict the use of deceased users' data for commercial purposes and ensure data anonymisation and aggregation in case it is used for research or model training. Directives by users over the disposition of their data after they die must be respected. When such data is necessary for the common good, say, in anonymous data sets linked with health research, companies must make sure tight security is in place and consider opting-in families or estates into decision-making.

SOCIAL CHALLENGES

Digital Grief and Mourning: Grieving has grown from physical spaces-home, cemetery, and community gatherings-into the digital era. Memorialised social media pages have transformed into virtual places of mourning, where friends and family, and even those who lived far from them, can state their condolences, share memories, and keep the presence of the deceased alive. These take the form of digital memorials in which photos, comments, and older posts serve as emotional anchors. These virtual spaces evoke in many, and particularly in those who cannot attend the physical services, feelings of participation and connectedness.

But mourning digitally is not homogeneous in its role. There are those for whom the constant vision of the profile of the deceased day after day could be wearing and might impede processes of healing. For every constant reminder birthday, memories, a surfacing post-it opens up old wounds rather than soothing them. At the same time, many indeed find substantial consolation in those digital remains. Reading the last conversations, looking at photos, or interacting with the memorialised page offers comfort, continuity, and a sense that the person is still present in some form.

Impersonation and Identity Theft: Another important challenge in the context of digital afterlife is constituted by the vulnerability of either inactive or unmonitored accounts, because such accounts are subjected to all kinds of malicious actors.

- To hack profiles and steal personal data.
- Create fake profiles in the identity of the deceased.
- Spread false information or political propaganda.
- Lie to family and friends for personal gain.
- Try fraud in the name of the victim.

Cultural and Religious Differences: Uniform digital afterlife management can never be possible as cultures and religious beliefs differ from one part of the world to another. In several cultures, the complete erasing of digital trails is crucial for spiritual peace or to avoid misuse of any kind. They look upon personal data as an extension of the human soul, and its preservation beyond life may be considered improper or spiritually harmful. Other cultures welcome remembering and honouring the dead. For such groups, sustaining the online profiles with uploaded photos, stories, and messages serves as a form of continuation to celebrate their lives and legacy. The memorial web pages become part of the cultural rituals of remembrance. Some religions also have severe restrictions on privacy, modesty, or the distribution of personal information. It would be inappropriate to allow the world free access to the personal information of the deceased in such cases, especially if it involves images or private messages. Because of this diversity, digital platforms need to consider developing policies that will be respectful, flexible, and sensitive to worldwide traditions. Ethical digital afterlife management has to consider that dying is not strictly a technological question but a cultural and spiritual one; therefore, thoughtful and culturally sensitive solutions must be found.

DIGITAL WILLS AND USER CONTROL

What is a Digital Will: The digital will names what happens with all online accounts, digital assets, and stored data when the owner is deceased. It's highly similar to a regular will but touches only on aspects of digital property, ranging from social media profiles and an e-mail account to cryptocurrency and cloud-stored photos. With the digital will, users can indicate who should get access to their data, manage or close accounts, and what information should be kept or destroyed forever.

Why do People need a Digital Will: This, if it were a digital will, would make much more sense, because the internet can barely be separated from personal identity or financial life, let alone emotional memory. In that respect, as soon as one dies, access to accounts usually becomes quite hard because the platforms require proof and legal documents and sometimes refuse completely on grounds of privacy. Without explicit instructions, families get locked out of crucial photos, messages, or even financial accounts.

Another significant reason is the prevention of misuse: unmonitored accounts can be hacked, impersonated, and used in scams. A digital will ensures that the accounts are memorialised, deleted, or transferred to persons of trust in good time; hence, the chances of cyber fraud are reduced.

Privacy protection also becomes a strong motivation whereby individuals do not want their family members to see some messages, emails, or documents. A digital will allows them to state which of these are to be kept confidential or deleted straight away. In the case of digital assets, financial or sentimental values are to their creators: writers, YouTubers, photographers, and gamers. The digital will ensures that this creative work is conserved and passed on to the right people. In the same way that owners should plan for the distribution of any cryptocurrency, NFTs, trading accounts, or online businesses, otherwise, heirs may lose access to these forever, given that crypto wallets cannot be recovered without keys. In summary, the digital will cuts down confusion; it leaves the dead with dignity intact and manages digital valuables responsibly.

Elements of a Digital Will: There are several elements that go into making a well-structured digital will. This would include, but is not limited to, all digital accounts, including social media platforms, email providers, cloud storage, banking apps, online subscriptions, e-commerce accounts, cryptocurrency wallets, and digital devices. This list becomes somewhat of a roadmap for the executor. The will should next indicate specific directions as to what shall happen to each account. For example, should the Facebook account be memorialised or deleted? Should email accounts be shut down or transferred to someone temporarily? Should photos stored in the cloud be shared with family or completely deleted? Clarity avoids confusion and, therefore, assures the executor of what is to be done. Another key component is naming a legacy contact or digital executor: trusted people who institute all the instructions written in the will and with whom online platforms converse and liaise. This does not grant this particular role owner access to all his or her data, except in those cases where such access has been given. Because it is unsafe to share passwords directly in a will, a digital will generally refers executors to a secure password manager, an encrypted document, or an attorney-managed key storage system. In the will, on the financial aspects of digital assets, it should be stated who gets what: crypto holdings, wallets, domain names, or monetised accounts, and how to access the same. Otherwise, such assets may become irretrievable. Lastly, there is a deletion preference in a digital will. Most people want certain documents, conversations, search histories or other files permanently deleted upon one's

death to protect dignity and privacy. Others may wish their sentimental items, such as photos or creative work, to stay for future generations. These put together make the digital will a potent tool through which one controls his or her digital legacy, protects privacy, and supports loved ones after death.

CASE STUDIES AND REAL EXAMPLES

Case Study 1: German Facebook Case: After a 15-year-old girl died, her parents wanted to see her messages on Facebook, but the site refused on the grounds of privacy. In this case, the German Federal Court decided that digital communications are inheritable just like a diary or letters, which established a global precedent for rights related to digital inheritance.

Case Study 2: Apple v Deceased Soldier's Family: Apple refused to unlock the iPhone of the soldier, which led the family into a legal battle. Only under a court order did Apple permit access, amidst a balance between strict protection of privacy and family rights.

Case Study 3: Celebrity Digital Legacy: Celebrities' social media often turns into a digital memorial that is maintained by families or estate managers after their death. Fans continue to interact, and revenue from music posts and digital content stays very much alive. Michael Jackson's digital estate still generates millions of dollars a year.

Case Study 4: Indian Scenarios. In India, families cannot access Google Photos, WhatsApp backups, or Facebook accounts of users who have died. Since there is no dedicated Indian digital inheritance law, all access depends on the policy a specific platform requires. On the question of legal support, the family has little.

CHALLENGES IN CREATING UNIFIED LEGAL RULES

Conflicting Values: The digital afterlife reflects values that are complex and in conflict. Probably the most strongly compelling principle involved is that of privacy. Personal messages, search histories, financial data, and all the other private conversations reflect a person's dignity and autonomy, including in death. Disclosure can be a serious breach of morals, since there is an expectation of confidentiality. Sometimes, families claim they need access for emotional

closure or to keep memories alive, so they must be given access to those accounts. Thus, direct opposition between privacy and the need for emotional closure arises.

Next come property rights. Digital accounts can include a variety of high-value assets: monetised YouTube channels, crypto wallets, digital art, manuscripts, or music. And the families would want to claim inheritance rights over such assets. The thing is, though, that platforms still view the accounts as licensed services and not property, which sets up some legal contradictions.

Ultimately, it is the cultural traditions that shape the expectations of how the dead should be treated. While some societies encourage the preservation of memories, others advocate for the complete deletion of data concerning the deceased. Inevitably, where these values overlap, there is going to be conflict. How they will balance these will call for nuanced laws, open policies, and further social understanding.

The Dominance of Technology Companies: What is perhaps most striking about digital afterlife management is how much power resides in the hands of companies. Unlike with physical property, digital assets are mostly subject to Terms of Service — corporate documents that nobody reads and whose existence one cannot negotiate. Tech platforms control everything:

- What data is stored?
- Where is it kept?
- How long is it kept?
- Who has control when someone dies?

Family members have no automatic right of access, even if they are legal heirs. Instead, they must follow the procedures laid down by the platform, most of which require a death certificate, identity documents, and a court order. And even then, the companies may decline service.

Strict control will be advantageous not only for individuals but also for companies. Making the data inaccessible would also enable them to continue the processing of such data for algorithm training or product improvement, if this is legally allowed. Such commercial interests may make platforms hesitant to supply or delete the data.

They will eventually become the gatekeepers of our digital afterlives and will decide the fate of millions of digital identities. If stronger regulations are not put in place, families will be thwarted by the obstacles, and society will be left at the mercy of their corporate whims.

Cross-Border Jurisdiction: Another complication is that digital data does not reside in any one location. An Indian resident may store information in a data centre in Singapore, the United States, or Ireland, thereby creating legal conflicts across borders.

For instance, European Union laws on privacy are among the strictest in the world. If a deceased user's data is housed in Europe, even non-EU families may have problems accessing it. American companies also abide by U.S. privacy laws, where the user's contractual relationship with the platform supersedes family claims.

Various countries also define differently:

- What is Digital Property?
- What heirs have access to?
- What privacy rights continue beyond death?
- What platforms are legally compelled to do?

It is when information of a dead man crosses boundaries that courts tussle to implement orders. Though the Indian court gives permission for accessing Google Photos to the family, the servers may come under U.S. law.

Data Persistence and Size: An average digital user leaves a huge, deeply intimate digital footprint. The typical footprint of any person would include:

- Thousands of photos stored on cloud platforms
- Years, even decades, of messages
- E-mails, from personal to professional contexts.
- Search histories
- Purchase records
- Medical Records
- Location histories

- Creative content
- Confidential conversations

Special challenges, both practically and ethically, arise in managing such voluminous data.

First, there is the volume of data; families often have no idea what they are inheriting or deleting. Tens of thousands of items can fit in one Google account - far too much for any one person to meaningfully review. This, in turn, makes posthumous decisions stressful.

Moreover, the sensitivity of the data amplifies the privacy concerns: the deceased might have had private relationships, confidential work files, or deeply personal messages never intended for the eyes of any other person. Full access to the families causes secrets to be exposed unwittingly, thus creating conflict or simply violating the dignity of the deceased.

Thirdly, digital data is permanent unless deleted. Deleted content may survive in some form as backups or archives. The permanency thereof invokes philosophical questions with regard to the persistence of someone's digital identity and for how long.

These digital footprints may be enormous in scale, and this in itself could make it hard for companies and families to treat data with respect and in order.

THE FUTURE: WHAT SHOULD BE DONE?

Importance of Clear Legislation: The confused and unclear laws of digital inheritance create a lot of confusion and emotional turmoil within the family, since physical and digital lives are becoming inseparable.[3] Most countries still retain outdated property laws that do not include a dead person's emails, cloud photographs, cryptocurrency, or social media accounts. Hence, there is an immediate need to draw up uniform and comprehensive digital inheritance laws. Such legislation would, among other things, need to state what digital assets are transferable, heirs are hereby recognised, and make sure that the deceased's privacy is protected. Well-laid-out

[3] Jonathan Ringel, 'Digital Inheritance Laws: Who Controls Your Social Media Legacy?' (*Story*, 07 July 2024) <https://www.storystreamline.com/law/digital-inheritance-laws-who-controls-your-social-media-legacy/> accessed 07 November 2025

legislation provides predictability, cuts down corporate arbitrariness, and ensures equal fairness in all cases, irrespective of the platform or country concerned.

Informed User Consent: Account management after death, in fact, includes setting legacy contacts, inactive account managers, and options for memorialization. Very few people in their lifetime think about their digital legacy, and the lack of planning at this juncture of life creates huge problems later on. There is, therefore, a need to educate users on these aspects and empower them in taking control over their digital afterlife. It is easy to set up settings on platforms so that people can decide what happens with their data, whether it has to be deleted, transferred to somebody they trust, archived, or memorialised. Clear consent mechanisms must be designed so as to have the wishes of users recorded legally and followed strictly. Encouraging people to make digital wills would also help their families avoid disputes and prevent identity theft or any other kind of data misuse.

Ethical AI & Data Use: With the rise of AI, companies collect and analyse large sets of data about users, including deceased ones. Such a situation then creates ethical risks when some platforms, without consent following a user's death, use such data for advertising, to train algorithms, or create strategies for engagement. This could be highly unethical, disrespectful, and exploitative. Companies do have a moral obligation and probably a legal one to ensure that once the person dies, the data isn't used for profit-making purposes unless explicit permission was granted. Ethics on data should place an obligation on platforms to stop feeding information of deceased users into the AI model, not allow unauthorised creation of “posthumous content,” and show clarity on the way data is stored or deleted. Human dignity remains at the core.

Open Platform Policies: Most of the policies at various platforms are written in complicated legal language that no ordinary user can understand. This sets a barrier for families knowing what their rights are, or how to request access upon the death of a loved one. Companies should institute simple, consistent, and fair policies clearly describing how digital assets will be treated. The procedures should be easy to follow, supported by step-by-step guidance, and be designed in such a way that they respect both privacy and inheritance needs. Full transparency will reduce confusion and inhibit companies from making arbitrary decisions.

Creation of Global Standards: Digital information moves across borders, and national laws are just not enough. A picture can be hosted in one country, the platform owning it registered in another, and the user's family lives in yet another. In that respect, what is needed are global standards guided perhaps by the United Nations or international digital rights bodies. Common principles regarding access to data, protection of privacy, verification of proof-of-death, and dispute resolution must form part of the standards. It would hence result in a uniform regime that ensures equity, cuts cases characterised by conflict, and provides a predictable framework within which to manage digital inheritance worldwide.

CONCLUSION: UNDERSTANDING AND MANAGING THE DIGITAL AFTERLIFE

One of the biggest and most complex questions for this modern technological era has something to do with the digital afterlife. As an increasing number of people are living their lives online, digital data-photos, messages, e-mails, cloud files, social media posts, financial accounts, and creative work have grown integrally with one's personal identity. The thing is, what happens to this identity upon a person's death? This is a question that requires an analysis premised on legal, ethical, emotional, cultural, and technological grounds.

The world is still pretty legally fragmented in a way that different countries treat digital data as something a person can or cannot inherit. Large platforms like Facebook, Google, Apple, and Instagram run on their own Terms of Service agreements, overriding traditional inheritance laws in so many cases. That's why so many families have problems trying to get access to their loved ones' accounts. Different courts of the world have passed judgments, but there hasn't yet been a comprehensive global legal framework. This creates tension for families and huge power in the hands of companies when it comes to digital legacy.

This is an ethical as well as it is an emotional quagmire because, many times, families want to see messages, photos, or cloud storage for memories or closure. Digital accounts of a child who has died may be possessed by things that mean something emotionally irreplaceable to parents. Yet, all privacy rights do not disappear at the time of death, and one may not want private conversations revealed, or personal material let out, even to the closest of family members. How these two competing sides of posthumous privacy and emotional needs can be balanced probably constitutes the most deep-seated ethical conflict in digital legacy management. From a cultural

and religious perspective, there is another layer. While some cultures give a high value to remembering the dead, others demand that personal information be taken off public platforms after death. A single-minded approach to digital policies pays no regard to such variable values. Digital afterlife management needs to be culturally responsive and adaptable to diverse belief systems. Technologically, the companies hold immense power in that, in most countries, user data resides on the companies' servers. This puts families at the mercy of the platforms for account access or deletion. Some companies also use the data from dead users to create analytics or for AI training without explicit consent. Important questions of dignity, autonomy, and ethics about posthumous usage of data lie here. Solutions to these problems demand a balanced approach: countries have to lay down specific legislation about digital inheritance that may define the rights and responsibilities; firms should provide users with transparent, easy-to-use legacy tools through which they can decide what happens with their accounts; and public awareness about digital wills and the planning of digital legacies is crucial. On the international plane, there needs to be cooperation because data crosses borders, and one country alone cannot regulate its flow. All in all, the digital afterlife reminds us that our online presence is much more than just data; it is a reflection of our relationships, memories, and identity. Managing such a legacy with clarity, compassion, and respect will ensure that the dignity of the dead is respected and the emotional needs of the living taken into consideration as humanely and responsibly as possible.