

PARADOX OF ENDURING IDENTITY: TOWARDS A POSTHUMOUS CONSENT GOVERNANCE APPROACH

✍ **Authors: Manisha Low, Nikhil Singh and Arjun Muraleedharan.**

ABSTRACT

History is marked by turning points that reshape the fundamentals of society. The Digital Revolution is one such turning point which challenged many of law's oldest assumptions. One of them is that death marks the end of legal personality and individual identity. But today, individuals' digital identities persist through online platforms, cloud archives, algorithmic profiles and AI systems that far outlive their creators.

This paper explores the legal discontinuity that emerges when personal data persist after the death of the individual whose consent authorized their processing. By adopting a doctrinal and comparative methodology, the study analyses statutory frameworks, judicial decisions and platform policies across multiple jurisdictions, integrates perspectives from privacy, succession, consent, data protection and platform governance. It identifies a conceptual discontinuity that arises when consent-based privacy governance outlives the individual whose consent originally authorized it, described in this paper as the Consent Extinction Gap. The findings indicate that although jurisdictions increasingly recognise posthumous digital rights, their responses differ significantly in legal foundations, allocation of decision-making authority and enforcement mechanisms.

This paper argues that contemporary privacy law requires a reconceptualization of posthumous governance of digital identities and provides a conceptual framework for addressing that challenge.

Keywords: Digital Afterlife; Post-mortem Privacy; Consent Extinction Gap; Digital Identity; Platform Governance; Data Protection; Digital Succession.

INTRODUCTION

Billions of individuals generate digital data daily through social media, email, financial transactions, health records and online activity. This digital data is collected silently throughout one's entire life, making the most complete and personal record of any individual ever created. But the moment one person passes away, an important legal question emerges – what happens to all this data and to whom it is accessible. And does the person who created it retain any rights over their own digital identity once they are gone?

These are not merely technical or legal questions, they are profoundly human ones. For grieving families, a deceased loved one's social media account may hold irreplaceable memories, private conversations or even clues about the circumstances of their death. For artificial intelligence companies, it is training material for chatbots, voice replicas, and digital avatars. The digital remains of the dead have simultaneously become objects of grief, commerce and technological development, yet the existing legal frameworks have struggled to keep pace.

The present paper is an analysis of one of the issues that have been widely neglected in modern legal discourse: right to privacy and right to control personal information in the post-mortem context. This issue is situated at the crossroads of constitutional law, data protection law, succession law and regulation of emerging technologies. Constitutional background of this research in India can be traced back to the unanimous Supreme Court judgement in *Justice K.S. Puttaswamy v. Union of India* (2017)¹, where the right to privacy was acknowledged as a fundamental right guaranteed by Article 21 of the Constitution of India².

India's attempt to address posthumous data rights through legislation has been partial at best. The Digital Personal Data Protection Act, 2023 (DPDP Act), brought into force in November 2025, introduces a nomination mechanism under Section 14³. Although it acknowledges posthumous decision-making, it leaves unanswered central legal question: what rights survive death and on what legal basis?

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

² Constitution of India, art. 21.

³ The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 14.

General Data Protection Regulation (GDPR) by the European Union, which is considered the strongest data protection regulation globally, expressly excludes the deceased from enjoying the rights afforded by it under Recital 27 and hence gives freedom to the member states to draft laws on the issue on their own accord⁴. France makes use of Article 85 of its Data Protection Act in providing an opportunity to an individual to provide directions for using or keeping or deleting his or her data after he or she passes away⁵. Germany's BGH in the 2018 Facebook Inheritance case ruled that digital accounts of the deceased fall into the category of inheritable estates and should be treated in the same manner as the letter or diaries in civil law⁶.

The contradictions within Indian law itself are striking. In *Krishna Kishore Singh v. Sarla A. Saraogi* (Delhi High Court, 2023), a case arising from the tragic death of actor Sushant Singh Rajput, the Court held unequivocally that the right to privacy, right to publicity and personality rights are personal rights that "died with his death" and were not heritable⁷. This constitutional position that privacy rights extinguish at death sits in direct and unresolved tension with the DPDP Act's nomination mechanism, which implicitly acknowledges that data rights can survive the person⁸. No Indian court has yet reconciled this contradiction.

Against this backdrop, this paper pursues three central objectives. First, it maps the existing legal framework consisting constitutional, statutory and judiciary that governs or ought to govern a deceased person's digital data in India, identifying the critical gaps that remain unaddressed. Second, it undertakes a comparative analysis of international frameworks including the GDPR regime, German civil law, French statutory protections and the US RUFADAA model, to draw lessons for Indian legislative reform. Third, it critically examines the social dimension of the problem: how platform power, AI exploitation, the behavioural paradox of digital legacy planning and the commercialisation of the digital afterlife industry together create a landscape in which the digital remains of ordinary people are left profoundly unprotected.

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Recital 27.

⁵ French Data Protection Act (Loi n° 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties), art. 85.

⁶ BGH (Federal Court of Justice, Germany), Judgement of 12 July 2018, Case No. III ZR 183/17 (Facebook Inheritance Case).

⁷ *Krishna Kishore Singh v. Sarla A. Saraogi & Ors.*, CS(COMM) 187/2021, Delhi High Court (2023)

⁸ Digital Personal Data Protection Act, 2023, s. 14.

The paper argues that posthumous privacy cannot be addressed solely through succession or data-protection law because both presume a living rights-holder. Instead, it proposes the Consent Extinction Gap as a conceptual framework for analyzing governance after the death of the data subject.

The law must evolve to reflect this reality. India, with over one billion internet users and a digital economy of growing global significance, cannot afford to remain silent on the rights of its citizens in the digital afterlife.

LITERATURE REVIEW

Privacy, Consent, and Digital Persistence:-

In current privacy scholarship autonomy and consent are seen as the key elements in the governance of personal data. Yet scholars like Solove and Nissenbaum have doubted whether consent by itself gives people meaningful control in relation to complicated data practices. Despite this, these approaches generally suppose the existence of a living data subject who is able to give or take back their consent.

Existing digital privacy research shows that social media profiles, cloud storage, emails, photos, biometric data, and algorithmically generated trails often persist beyond biological death, creating lasting digital identities. These digital traces serve as places for memory, mourning, and identity preservation. Edwards and Harbinja look at how social-media accounts and digital assets persist and are passed on, while Harbinja and Maciel and de Paula focus on post-mortem privacy and the digital afterlife. Although this body of literature confirms the persistence of digital identity it pays comparatively less attention to the governance implications resulting from the disappearance of the original consent-holder.

Platform Governance and Posthumous Authority:-

Technology platforms increasingly set rules for digital death through memorial policies, legacy contact systems, inactive account managers, and deletion processes. Studies of these practices show that platforms play a growing role in governing digital remains.

However, these governance practices shift authority. Decision-making often moves from the deceased individual to family members, legal representatives, or platform administrators. While research acknowledges this shift, it seldom investigates whether these arrangements maintain the autonomy of the deceased or simply replace it with the interests of surviving individuals and institutions.

Posthumous Privacy and Emerging Legal Challenges:-

Different legal approaches show various methods of granting posthumous authority –

- In Germany the decision concerning Facebook accounts was based on succession law,
- In the United States RUFADAA uses a fiduciary-access approach,
- In France it is possible to give posthumous instructions with regard to personal data.

It is clear from these examples that the main question is not simply whether posthumous rights exist, but who is given the authority and on what legal basis.

AI-Mediated Digital Resurrection:-

Recent advances in artificial intelligence complicate posthumous privacy governance further. AI can now create conversational agents, virtual avatars, and synthetic personalities based on the digital footprints of deceased individuals.

Existing research mainly addresses ethical issues around authenticity, grief exploitation, emotional reliance, and commercialization, while the question of consent following the loss of agency is comparatively little explored.

Critical Synthesis:-

The literature thus shows four related areas: privacy and consent, the digital afterlife, digital inheritance, and platform/AI governance. However, these areas are still not sufficiently integrated. The work in the field of privacy is concerned with the living individual; research into the digital afterlife deals with persistence; succession law is concerned with the redistribution of authority; and the platforms are now exercising actual control. What has not been adequately addressed is an integrated explanation of how consent-based governance can be considered legitimate when the autonomous person who gave the consent ceases to exist permanently. It is this unresolved point of intersection that forms the foundation of the current study.

Research Gap:-

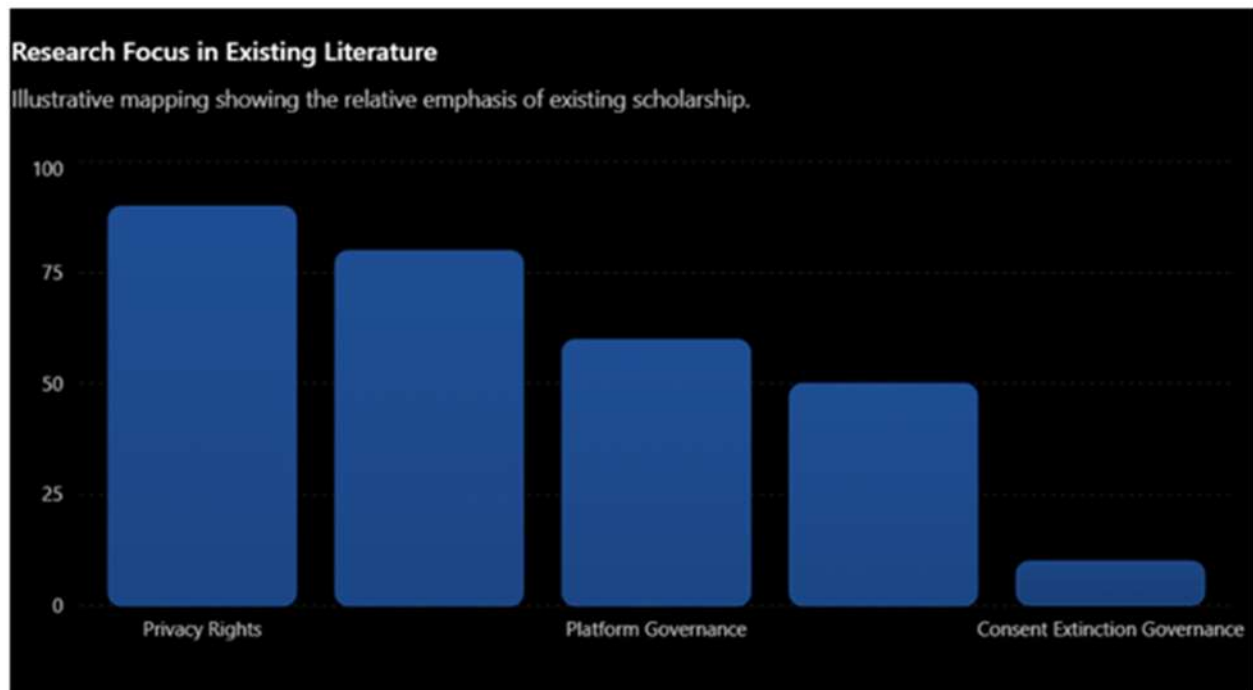
The current body of research shows that digital identities continue to exist after a person has died and that mechanisms for dealing with them have arisen. Yet there is still a conceptual gap at the point where consent, autonomy and posthumous governance meet.

Privacy models that are based on consent usually suppose a living person who is able to give or take back their consent. Most of the research carried out after a person's death is concerned with protecting or obtaining access to the data of the deceased, whereas succession and fiduciary models involve the redistribution of authority without necessarily respecting the deceased's preferences. Moreover, the governance practices of platforms and AI allow private individuals to take control of or rebuild digital identities following the loss of an individual's agency.

This study refers to the condition as the Consent Extinction Gap: it is a scenario where the original data subject can no longer grant, amend, revoke or challenge their consent, even though their personal data or digital identity still exists and remains under the control of others.

The concept is different from post-mortem privacy since it specifically deals with the discontinuity between ongoing data governance and the disappearance of the individual who originally gave consent. It also differs from digital inheritance, which mainly involves the transfer or administration of digital assets.

The study looks at the lack of discussion in the existing body of scholarship regarding the legitimacy of consent-based governance after the original autonomous data subject ceases to exist; the proposed Posthumous Consent Governance Framework (PCGF) deals with this gap by viewing death as a kind of transition in the field of governance rather than just the end of the data subject's status.



RESEARCH METHODOLOGY

Research Paradigm and Philosophical Position

This study takes an interpretivist socio-legal research approach supported by a critical governance perspective. The interpretivist approach is fitting because the main ideas explored in this study consent, autonomy, privacy, digital identity, and death are shaped by social and legal contexts rather than being fixed. Their meanings arise from legal frameworks, technological setups, institutional practices, and socio-cultural views.

At the same time, a critical governance perspective allows for an analysis of how control over personal data changes after a person's death. This study starts from the idea that digital death is

not just a biological event but a change in governance. In this transition, personal data, digital identities, and algorithmic representations continue to exist even after the individual, whose autonomy legitimated their use, has gone.

Thus, the research aims to understand how modern governance systems react when digital existence continues after biological life ends.

Research Design

The study uses a qualitative, exploratory, comparative, and theory-building research design.

An exploratory design is suitable because posthumous digital autonomy is a new area filled with conceptual confusion, scattered regulations, and little theoretical agreement. Previous studies have looked at privacy rights, digital legacy, platform governance, and AI-driven digital resurrection separately. However, there has been limited investigation into how these areas intersect concerning posthumous consent governance.

Instead of just pointing out regulatory gaps, this study aims to create a conceptual framework that explains how governance authority shifts when the original data subject is no longer present. Therefore, the research goes beyond mere description and contributes to theory development in posthumous privacy governance.

Research Objectives

The study seeks to:

- Examine how current privacy and data governance frameworks view consent, autonomy, and privacy concerning deceased individuals.
- Analyze how digital platforms manage posthumous digital identities through memorialization, legacy access, and account management systems.
- Investigate how AI-driven digital resurrection technologies challenge existing consent-based governance models.

- Identify governance issues that arise from losing active consent after death.
- Develop a theoretical framework for posthumous consent governance in a world with persistent digital identities.

Research Strategy

To address the research objectives, the study employs a four-stage analytical plan.

Stage I: Doctrinal Legal Analysis

The first stage involves a thorough examination of legal and regulatory frameworks surrounding personal data and privacy.

Primary sources include:

1. Digital Personal Data Protection Act, 2023 (India)
2. General Data Protection Regulation
3. Judicial decisions related to privacy, dignity, autonomy, informational self-determination, and posthumous rights
4. Government consultation papers and policy documents

The analysis will focus on:

1. Definitions of consent
2. Recognition of data subjects
3. Continuity of privacy rights after death
4. Treatment of posthumous data
5. Allocation of authority over digital remains
6. Legal basis
7. Allocation of authority
8. Scope
9. Practical effectiveness

The goal is to see if existing legal frameworks establish a clear connection between biological death and digital persistence.

The study looks at legislation, judicial rulings, regulatory documents, academic literature and the policies of the platforms. The comparative sample includes jurisdictions which have been selected on the basis of their legal relevance, the variation in the approaches taken, comparative importance and the availability of reliable primary sources. Special attention is paid to the EU/GDPR framework, Germany, France, the United States and India since these countries embody different approaches to posthumous digital governance.

The United States is also looked at in respect to the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) and the way it has been put into effect in 53 jurisdictions.

Stage II: Platform Governance Analysis

The second stage looks at how major digital platforms manage deceased users' digital identities.

Policy documents related to the following platforms will be analyzed:

- Meta Platforms
- Google
- Apple

The analysis will examine:

1. Memorialization procedures
2. Legacy contact systems
3. Account deletion processes
4. Successor authority
5. Data access rights
6. Institutional views on posthumous autonomy

This stage allows for a comparison between public regulatory governance and private platform governance.

Stage III: AI-Mediated Digital Afterlife Case Analysis

The third stage includes qualitative analysis of documented cases involving AI-generated representations of deceased individuals.

Cases will be chosen based on the following criteria:

1. Use of data belonging to deceased individuals
2. AI-based personality simulation or interactive conversation
3. Ethical, legal, or governance significance
4. Availability of documented evidence

Examples include AI grief bots, digital resurrection systems, AI memorial applications, and synthetic identity reconstruction technologies.

This stage investigates how new technologies change digital remains from passive archives into active digital entities and how these changes challenge traditional views of consent and autonomy.

Stage IV: Expert Validation (Optional)

To improve analytical validity, semi-structured interviews may be conducted with:

1. Privacy law scholars
2. Digital rights researchers
3. AI ethics experts
4. Platform governance specialists

The interviews will explore:

- The conceptual limits of consent after death
- Governance challenges related to persistent digital identities
- Regulatory responses to AI-mediated digital resurrection

- Future directions for posthumous privacy governance

The goal of this stage is to validate emerging theoretical insights rather than achieve statistical generalization.

Data Collection and Sampling Strategy

The study uses purposive and criterion-based sampling.

Documents, policies, and case studies will be chosen based on the following criteria:

1. Relevance to consent-based governance
2. Engagement with posthumous privacy issues
3. Discussion of digital identity persistence
4. Relevance to AI-mediated digital afterlife
5. Regulatory or governance importance

This sampling strategy ensures analytical relevance while keeping a clear focus across datasets.

Data Analysis

The study uses a multi-layered analytical framework with thematic analysis and critical discourse analysis.

The Consent Extinction Gap is defined by three conditions:

1. the death of the individual in question;
2. the continued existence or use of the person's personal data or digital identity; and
3. the data being governed by parties other than the original individual.

Thematic Analysis

All collected materials will be systematically coded and categorized.

Initial coding categories include:

1. Consent
2. Autonomy
3. Privacy
4. Digital identity
5. Data persistence
6. Informational personhood
7. Legacy governance
8. Successor authority
9. Platform responsibility
10. AI-mediated identity reconstruction

Through iterative coding and interpretation, broader themes and conceptual relationships will be identified.

Critical Discourse Analysis

Critical discourse analysis will be used to explore how governance systems linguistically represent the deceased individual.

Special attention will be given to:

- Recognition of agency
- Construction of authority
- Allocation of rights
- Assumptions about ownership of digital remains
- Governance narratives surrounding death and data

This method helps identify hidden assumptions and power structures found within legal and technological governance systems.

Operationalization of the Central Concept

To ensure analytical clarity, the study defines Consent Extinction as:

The situation where the original data subject cannot grant, modify, withdraw, or contest consent, while their digital identity, personal data, or algorithmic representations persist and remain subject to governance decisions.

A situation will be classified as a Consent Extinction Scenario when the following conditions occur together:

1. Biological death of the data subject.
2. Continued existence or use of personal data.
3. Governance decisions made by others rather than the original data subject.

This definition provides a structured basis for analysis and strengthens methodological thoroughness.

Conceptual Framework: Posthumous Consent Governance Framework (PCGF)

The study proposes a new model called the Posthumous Consent Governance Framework (PCGF).

This framework views the posthumous data lifecycle as:

Biological Death → Consent Extinction → Persistence of Digital Identity → Redistribution of Governance Authority → AI-Mediated Identity Continuation → Governance Legitimacy Challenge

The framework aims to explain how governance systems strive to keep legitimacy when the autonomous subject who originally provided consent is no longer available.

Within this framework, the study introduces the Consent Extinction Principle (CEP):

When the autonomous subject no longer exists but the digital identity remains, governance authority inevitably shifts to secondary actors, leading to a legitimacy-gap in consent-based privacy systems.

This principle serves as the study's main theoretical proposition.

Reliability, Validity, and Trustworthiness

To ensure methodological rigor, the study will use:

- Source triangulation across legal, technological, and academic materials.
- Cross-validation between legal frameworks, platform policies, and case studies.
- Clear coding procedures.
- Reflexive analytical documentation.
- Comparative interpretation across governance systems.

These measures strengthen credibility, dependability, and theoretical strength.

Ethical Considerations

The study will follow principles of academic integrity, confidentiality, and responsible scholarship. No personal data from deceased individuals will be collected or processed. If expert interviews are conducted, informed consent, voluntary participation, anonymity, and secure data handling procedures will be upheld.

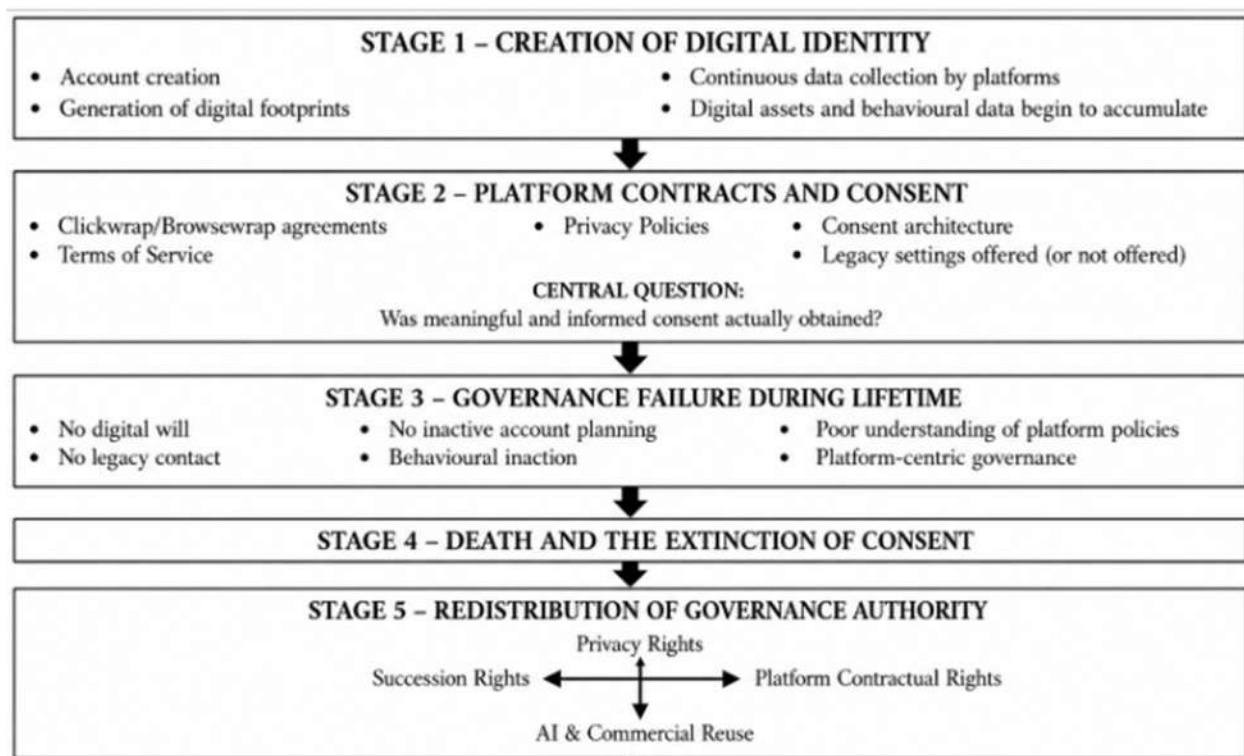
Expected Scholarly Contribution

This study asserts that the main challenge of posthumous privacy lies not just in the persistence of data after death but in the persistent governance obligations that remain after the autonomous subject has ceased to exist.

By developing the Posthumous Consent Governance Framework (PCGF) and the Consent Extinction Principle (CEP), the study aims to provide a new theoretical perspective on privacy, autonomy, governance legitimacy, and digital identity in a time when digital existence often outlasts biological life.

CASE STUDY FRAMEWORK

This proposed framework traces the evolution of an individual's digital identity through five stages.



Stage 1: Creation of Digital Identity

Through continuous usage of digital platforms, individuals build their digital identities by generating personal data. Emails, social media posts, photos, geolocation data, online transactions, biometric records are all spread across platforms, databases, cloud storage services, financial institutions, artificial intelligence systems.

Floridi describes this as the emergence of the “infosphere”, where the distinction between the physical and digital worlds is getting blurred⁹. He argues that humans are no longer merely biological entities, but also informational entities whose identities are continuously shaped by the

⁹ Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press, 2014).

production, exchange and processing of information¹⁰. Digital identity is not just an extension of the individual, but is an integral component of their personhood. As personal data is closely tied to an individual's autonomy, dignity, and self-determination, interference with it gives rise to legal concerns.

Mayer-Schonberger argues that modern technologies have fundamentally altered the traditional balance between remembering and forgetting¹¹. Historically, forgetting functioned as a natural limitation on the accumulation of personal information, allowing individuals to evolve beyond past actions and experiences. But now, digital technologies make permanent retention the default and deletion the exception. Even where users attempt to erase information, copies may persist in backups, cloud servers, cached pages, algorithmic archives, third-party repositories.

Creation of digital identity marks the beginning of a legal relationship between individuals and digital platforms that persists throughout life and extends beyond death.

Stage 2: Platform Contracts and Consent

This legal relationship is formed through standard form electronic contracts, like click-wrap agreements, browse-wrap agreements, Terms of Service (ToS), and privacy policies. Users are typically presented with lengthy, complex, non-negotiable terms on a “take-it-or-leave-it” basis, through which platforms obtain users’ consent to collect, process, retain and govern users’ digital identities.

Solove argues that modern privacy regulation relies excessively on “privacy self-management”, assuming that individuals are capable of making informed decisions on complex data-processing practices¹². But in reality, as Hartzog rightly points out, users lack time, expertise and patience to evaluate such intricate contractual arrangements¹³.

¹⁰ *Ibid*

¹¹ Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).

¹² Daniel J. Solove, “*Privacy Self-Management and the Consent Dilemma*” (Harvard Law Review, 2013).

¹³ Woodrow Hartzog, *Privacy's Blueprint* (Harvard University Press, 2018).

Despite such limitations, these contracts continue to serve as principle mechanism for obtaining users' consent, providing legal basis for consent-based digital governance, which initially appears sufficient because it rests on users' contractual consent.

Stage 3: Governance Failure During Lifetime

The resulting wrap-contracts fail to secure meaningful and informed consent. Users neither read nor fully comprehend the legal consequences of the terms they accept¹⁴. Governance of an individual's digital identity begins not with a statutory framework, but with a private contractual framework drafted unilaterally by platform providers.

When creating an account, users are rarely required or encouraged to make informed decisions about the future of their digital identities after their death. Google's Inactive Account Manager, Facebook & Apple's Legacy Contacts etc. are optional features which are voluntary, unknown, poorly understood and extremely underutilized. Most major digital platforms' contractual provisions either terminate deceased users' accounts or reserve broad discretion over their data management, enabling platforms rather than users to determine future governance of their digital identities. Many ToS expressly deny any right of survivorship, which rules out succession rights. Governance begins to diverge from the users' continuing autonomy long before death occurs; and death transforms this gradual divergence into a complete legal discontinuity.

Stage 4: Death and the Extinction of Consent

Consent is assumed to originate from a living legal subject capable of exercising autonomy. But even after death of the capable living legal subject, the informational subject not only persists, but continues to be stored, processed, shared, commercially exploited, and also remains vulnerable to identity theft.

¹⁴ Nancy Kim, *Wrap Contracts: Foundations and Ramifications* (Oxford University Press, 2013).

This discontinuity is the Consent Extinction Gap, which necessitates a redistribution of governance authority.

Stage 5: Redistribution of Governance Authority

Governance authority over the deceased users' digital identity becomes fragmented among competing actors –

- Heirs seeking access to digital accounts as part of the deceased's estate;
- Platforms relying on contractual terms and ToS;
- Commercial actors seeking reuse of personal data through digital replicas, grief-bots etc.

Their claims are further complicated by privacy principles which favour protection of deceased's' confidentiality.

None of the actors can assume absolute governance authority, and so the digital identity survives as an object of legal, contractual, commercial, and governance interest.

KEY FINDINGS

The case study framework that has been adopted initially in the study highlights that postmortem digital privacy disputes are life cycle governance failures. The life cycle perspective suggests that disputes relating to data privacy of the dead ones originate during an individual's interaction with digital platforms during the lifetime of the individuals. Governance failures amid digital contractual arrangements during the user's lifetime itself are major causes. Lack of guidance during digital interaction to the users end in unknowingly acceptance of click wrap agreements, privacy policies, and terms of service. Fewer platforms provide limited guidance with respect to the management of digital assets after death. Inadequate digital estate planning, low awareness of legacy tools, and platforms and data governance further amplify the issue. Consequently, legal conflicts arise after death. This highlights the need for stronger consent mechanisms, greater platform accountability, and proactive digital legacy planning alongside legislative reforms.

Based upon the insights from case study framework, the study further aims to comprehensively review and assess the legislative ecosystem regarding Post mortem digital privacy disputes.

The first objective of the study intends to comprehensively compare the privacy laws existing in legislations/countries, divided across four regions. All the countries in the dataset have data protection or privacy legislation in force. It confirms that Existence of the privacy laws is no longer the matter of concern across major economies.

The second objective of the study examines the maturity level if the US digital-afterlife framework. The analysis covers the 53 jurisdictions across US, 92.5% of which have enacted, introduced in 1 and 3 are yet to enact the Revised Uniform Fiduciary Access to Digital Assets Act (2015). The four non enactors include Delaware, Louisiana, Puerto Rico, and Massachusetts. However, Delaware has kept the older 2014 version of legislations; Louisiana and Puerto Rico show no record of acting on either version; Massachusetts has only introduced a bill.

The third objective of the study involves critically appraising the enforcement of GDPR Article 17 across European Union, further analyzing if this article is enforced evenly or not. The findings from the analysis of 131 GDPR Article 17 enforcement actions 2019 to 2026 underscores that right to erasure is actively being enforced across Europe. However, it varies considerably across jurisdictions. Highest numbers of cases have been recorded from Italy (30 cases), Spain (25), and Romania (24) but the imposition of average fines is relatively modest. France extracted largest total fines (€63.05 million) only from 6 cases, largely due to CRITEO penalty. Clearview AI and Google LLC were repeatedly fined across separate jurisdictions for substantially the same conduct.

Fourth objective assesses the trend of the enforcement frequency and checks if the volume predicts severity. Empirical findings indicate stable enforcement activity despite year-to-year fluctuations. Further not statistically significant trend is observed in annual case volumes (slope of -0.35 cases/year, R^2 being the 0.013 and p -value of 0.789), suggesting no increase or decrease in enforcement frequency. Despite this, the cumulative fines rose sharply to €126.4 million by 2023 mainly due to exceptionally large penalties after 2021. Statistically there exist no significant relationship between case volume and average fine severity across all countries ($r = -0.133$, $p = 0.714$). France being an outlier where there is significant positive correlation ($r =$

0.715, $R^2 = 0.512$, $p = 0.030$). Nevertheless, given the limited sample size, this relationship should be interpreted cautiously and considered indicative rather than conclusive.

Fifth and the final objective of the study assess the India's DPDP Act stand in posthumous data governance framework. The comparison of the India's Digital Personal Data Protection (DPDP) Act, 2023 indicates that the legislation is a limited though progressive approach to digital afterlife rights. Section 14 of the DPP rules, which later came into force on 14 November 2025, extended a provision to authorize a nominee who can exercise deceased's' data rights, including the provisions related to correction and erasure. The US's RUFADAA on the other side grants fiduciaries broad access to digital accounts and content, which is in force state by state. France's Loi pour une République numérique alternatively recognizes comprehensive Heir rights and posthumous digital instructions. India's framework on the contrast remains confined to rights administration. India is the first south Asian jurisdiction to formally recognize posthumous data rights. However, these legislations are narrower in scope where practical effectiveness can't be assessed due to the absence of enforcement experience.

DISCUSSION

The dead leaves enormous data in form of extensive, permanent digital trail emails, social accounts, cloud photos, financial and behavioral data. Right to privacy to this data remains a concern within the digital privacy framework. The governance of this afterlife data has emerged as a significant challenge for privacy law, as traditional legal principles were not designed to address the continued existence of personal data after death. Postmortem digital privacy is a lifecycle governance issue, which is much bigger than merely a legal problem that begins posthumously. Issues related to the digital identity and data privacy arise account creation, electronic contracting, and governance failures throughout an individual's lifetime. Individuals tend to accept digital platforms' terms and conditions without meaningful consent, as they rarely engage in digital estate planning. These unresolved data governance issues pertaining to the data become legal disputes after death involving privacy, succession, and platform related rights. There is the big question with respect to the rights of the person who generated to the data when alive, what the literature terms it as 'digital afterlife'. There exist the legislations across the

world governing the data of the dead ones. The current article examines the right to privacy for the dead and control over personal data in the digital afterlife and rights in digital times.

The findings have revealed that there exists afterlife data protection legislation across major economies. This implies that having a privacy law is now the norm, not the exception, among major economies; the open question has shifted to enforcement and what happens after death.

92.5% of jurisdictions in the U.S. have enacted RUFADAA, making it the country where legislation is the broadest in terms of application. This is one of the rare areas of US law approaching near-total state-level consensus. RUFADAA grants fiduciaries access to a deceased person's digital accounts, yet this law is designed to fail, as it provides fiduciary access but does not provide any privacy rights to the deceased person, while platform compliance is irregular and varies from state to state with no federal override.

The French Article 85 framework is conceptually better since it allows users to determine their advance directives before death and considers posthumous regulation as an extension of lifetime autonomy. Still, it is not effective due to low user engagement and most people do not use the opportunity to exercise these rights.

Germany's BGH decision (2018) has been the best one doctrinally since it equated social network accounts to letters and diaries in terms of inheritance. Still, even this breakthrough is not practically significant since compliance by Facebook gave a 14,000 page-long PDF that is difficult to use by the family of the deceased person.

India is at the very beginning point. India has introduced a narrow "nomination" right (Section 14, in force Nov 2025), a first for South Asia. It's the first legislative step by India surrounding infrastructure implementing rules, and regulatory guidance. It is comparatively narrower in scope than France and US. When tested on the criteria of its peers, the effectiveness of the provision is severely hampered because the provision fails to state what rights would the nominee hold and also lacks enforceable obligations on the part of the platforms and any integration of the provisions with the Indian Succession Act of 1925. Most importantly, the provision is in direct conflict with the decision given in the case of Krishna Kishore Singh vs. Sarla Saraogi (2023) by the Delhi High Court, which stated that the privacy rights cease upon the death of a person which is a constitutional paradox in itself.

Overall, the findings indicate that posthumous digital privacy is evolving into an essential component of modern data governance. Policymakers should move beyond merely recognizing the posthumous rights over the data and work towards developing a comprehensive governance framework defining the roles of individuals, stakeholders, regulators, and platforms clearly in governing the afterlife data.

CONCLUSION

This research draws attention to an important contradiction between individual autonomy and digital identities governance in the post-death context. It is clear that the established frameworks of consent used in the current regulation and digital practices are incapable of handling the permanent and replicated nature of information online, thus generating a so-called “consent extinction gap.”

In general, the research shows a tendency towards the power transition from individuals to different platforms and other stakeholders once the person becomes either digitally dead or completely inactive. The results indicate serious issues related to privacy, data ownership, and ethical data management in the context of digital afterlife. The posthumous power transition raises serious questions regarding the relevance of the concept of consent as it is developed for living people.

Therefore, it becomes evident that there is an urgent need for revising the existing legal and ethical frameworks in order to take into account the issue of digital footprint persistence beyond physical life.

The proposed Posthumous Consent Governance Framework (PCGF) can be incorporated into future legislative reforms by allowing individuals to record their posthumous preferences regarding their digital data and by clearly defining the roles of nominees, heirs, platforms, and regulators. Such reforms should establish enforceable procedures for implementing these preferences and resolving disputes over posthumous digital rights. This would translate the PCGF from a conceptual model into a practical framework for governing digital identities after death.

LIMITATIONS

The conceptual framework proposed in this study remains theoretical. Its explanatory value across different jurisdictions and institutional settings requires future empirical testing.

First, jurisdictional selectivity necessarily constrains the comparative analysis. This paper draws on legal frameworks from the European Union (GDPR), Germany (BGH Facebook Inheritance Case, 2018), France (Article 85, Data Protection Act), and the United States (RUFADAA), a truly exhaustive global survey. The comparative analysis though, is limited to jurisdictions selected for their doctrinal influence on digital privacy and succession. Other jurisdictions with developing posthumous data regimes fall outside the scope of this study.

Second, legislative fluidity poses a significant challenge to the stability of the paper's conclusions. The Digital Personal Data Protection Act 2023 remains only partially enforced, having had the DPDP Rules 2025 notified in November 2025 while the rest of the provisions of the Act are set to become enforceable from May 2027 onwards. Consequently, conclusions regarding the DPDP Act's practical operation remain predictive rather than evaluative.

Third, this paper relies primarily on doctrinal and secondary research. It does not incorporate primary empirical data such as surveys of platform practices, user behaviour studies or interviews with legal practitioners and families navigating posthumous data access. The behavioural dimension of digital legacy planning particularly the documented gap between awareness and action identified in the literature would benefit from original empirical research in the Indian context.

Given the interdisciplinary scope of the study, individual doctrinal issues are addressed only to the extent necessary to develop the proposed conceptual framework.

SCOPE FOR FUTURE RESEARCH

The gaps identified in this paper open several productive avenues for future scholarly and legislative inquiry:

1. The most immediate need is for India to develop a coherent Digital Succession Law, one that integrates the DPDP Act's nomination mechanism with the Indian Succession Act, 1925, clearly defines the legal status of digital assets as inheritable property, and provides enforceable obligations on platforms.
2. Future research should directly examine the constitutional question left unresolved by Krishna Kishore Singh (2023) whether fundamental rights under Article 21, including the right to privacy, can be extended posthumously by statute and whether such extension would survive constitutional scrutiny.
3. Empirical research is needed on how Indian platforms particularly domestic social media and fintech companies currently handle deceased users' data in the absence of legal mandates.
4. The intersection of AI regulation and posthumous data rights deserves dedicated scholarly attention. As India's proposed Digital India Act takes shape, it must explicitly address the use of deceased individuals' data in training generative AI systems, an area where no global legal framework currently provides meaningful protection.
5. Does the Consent Extinction Gap explain judicial outcomes across jurisdictions?
6. Can the PCGF predict platform governance decisions?
7. Does CEP improve legal reasoning compared with existing privacy theories?

Finally, comparative research examining how personal law frameworks such as Hindu Succession Act, Muslim personal law, Indian Christian Marriage Act interact with digital succession rights could reveal important inequalities in posthumous data protection across different communities.

The section identifies several worthwhile avenues for legislative and doctrinal development. However, it would benefit from distinguishing policy recommendations from research questions and from outlining how the conceptual framework proposed in this article may be empirically or comparatively evaluated. Future research should evaluate whether the Consent Extinction Gap provides a useful conceptual framework for understanding posthumous governance across legal systems and emerging AI technologies.

ACKNOWLEDGEMENT

We sincerely acknowledge the contributions of our fellow intern, **Aryan Gaba**, whose support and dedication greatly enriched this research project.

REFERENCES

Academic Journal Papers:

1. Edwards, L., & Harbinja, E. (2013). What Happens to Our Social Media Accounts When We Die? *Information & Communications Technology Law*, 22(2), 133–144.
2. Lilian Edwards & Edina Harbinja, Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World, 32 *Cardozo Arts & Ent. L.J.* 83 (2013).
<https://larc.cardozo.yu.edu/cardozoelj/vol32/iss1/5/>
3. Edwards, L., & Harbinja, E. (2013). What happens to my Facebook profile when I die? Legal issues around transmission of digital assets on death. In C. Maciel & V. Pereira (Eds.), *Digital Legacy and Interaction: Post-Mortem Issues* (pp. 115–144). Springer.
https://doi.org/10.1007/978-3-319-01631-3_7
4. Harbinja, E. (2017). Post-mortem privacy 2.0: theory, law, and technology. *International Review of Law, Computers & Technology*, 31(1), 26–42.
<https://doi.org/10.1080/13600869.2017.1275116>
5. Maciel, C., & de Paula, B. (2018). Digital Afterlife and Posthumous Privacy: Ethical and Legal Challenges. *AI & Society*, 33(3), 425–433.
6. Mayer-Schönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*, Princeton: Princeton University Press, 2011.
<https://doi.org/10.1515/9781400838455>
7. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
https://hci.stanford.edu/courses/cs047n/readings/Privacy_in_Context.pdf

8. van Dijck, Jose, The Culture of Connectivity: A Critical History of Social Media (New York, 2013; online edn, Oxford Academic, 24 Jan. 2013).
<https://doi.org/10.1093/acprof:oso/9780199970773.001.0001>

Report/Institutional Paper:

9. United Nations Conference on Trade and Development (UNCTAD). (2021). Data Protection and Privacy: The Global Framework.
<https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide#>
10. World Economic Forum. (2020). Rethinking Data Ownership in the Digital Age.

Legal / Policy Sources:

11. Constitution of India, art. 21.
12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
13. Krishna Kishore Singh v. Sarla A. Saraogi & Ors., CS(COMM) 187/2021, Delhi High Court (2023)
14. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), especially Section 14 (Nomination Mechanism) and Section 4 (Processing of Personal Data)
<https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
15. Ministry of Electronics and Information Technology (MeitY), Digital Personal Data Protection Rules, 2025 (Notified November 2025)
<https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa>
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union.
17. Revised Uniform Fiduciary Access to Digital Assets Act (2015) (United States).

18. French Data Protection Act (Loi n° 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties), art. 85.
19. BGH (Federal Court of Justice, Germany), Judgement of 12 July 2018, Case No. III ZR 183/17 (Facebook Inheritance Case).
20. The Information Technology Act, 2000 (Act No. 21 of 2000)
https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
21. The Indian Succession Act, 1925 (Act No. 39 of 1925)
https://www.indiacode.nic.in/bitstream/123456789/19051/1/indian_succession_act_1925.pdf
22. Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press, 2014)
<https://www.oii.ox.ac.uk/research/publications/the-fourth-revolution/>
23. Solove, Daniel J., Privacy Self-Management and the Consent Dilemma (November 4, 2012). 126 Harvard Law Review 1880 (2013), GWU Legal Studies Research Paper No. 2012-141, GWU Law School Public Law Research Paper No. 2012-141, Available at SSRN:
<https://ssrn.com/abstract=2171018>
24. Hartzog, Woodrow, "Privacy's Blueprint: The Battle to Control the Design of New Technologies" (2018). Books. 334.
<https://scholarship.law.bu.edu/books/334>
25. Kim, Nancy S., Wrap Contracts: Foundations and Ramifications (September 7, 2013). Oxford University Press, Forthcoming, Available at SSRN:
<https://ssrn.com/abstract=2322255>