Digital Legacy Governance: Exploring a Chinese Path under the Civil Code in Light of International Models

Han Chen

School of Finance, Shanghai University of Finance and Economics, Shanghai, China

2023121529@stu.sufe.edu.cn

Abstract. Digital legacy indicates the bundle of accounts, data and digital assets that continue to exist after a natural person's death. This paper addresses three questions: what policy-ready definition and taxonomy of "digital legacy" best guide governance; how comparative regimes perform in practice; and what China-specific pathway under the Civil Code of the People's Republic of China (CCPRC) can effectuate user intent, protect post-mortem dignity and third-party privacy, and enable lawful succession at scale. Using a comparative doctrinal and policy-analysis approach, the study triangulates primary legal sources (statutes, regulations, case law), official platform documentation and 2022-2025 peer-reviewed scholarship. It first consolidates a functional taxonomy spanning direct-value digital assets, derivative-value accounts and sentimental/cultural records. It then synthesizes international experience: the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) authority hierarchy in the United States; the EU's exclusion of deceased persons in General Data Protection Regulation (GDPR) paired with Member-State rules (e.g., France's post-mortem directives); Germany's inheritable-contract doctrine; evolving industry guidance; and heterogeneous platform tooling (designation, memorialization, export and scoped access). Building on these findings, the paper proposes a China roadmap that clarifies concepts and authority, mandates privacy-preserving, auditable disclosure via standardized evidence packages and Application Programming Interfaces (APIs), and scales pre-death designations through usable defaults. The contribution is a layered governance model—statutory baselines, standards, platform implementation and user planning—that is legally coherent, operationally feasible and culturally sensitive.

Keywords: Digital legacy, post-mortem privacy, fiduciary access, platform governance, Civil Code of the People's Republic of China (CCPRC).

1. Introduction

Everyday life is now digital-by-default, and the breadth of what people leave behind online is easy to underestimate. Social presence alone spans the majority of humanity: as of July 2025, there are an estimated 5.41 billion social-media user identities—roughly 65.7% of the world's population—an indicator of how widely an individual's traces are dispersed across providers and jurisdictions [1]. These "user identities" are not guaranteed to map one-to-one to unique persons, but capture the scale of the repositories that persist after death and must be governed. At the same time, provider housekeeping rules can reshape what actually survives: for example, Google's two-year inactivity policy allows deletion of an unused account and its contents, unless the user has configured Inactive Account Manager (IAM) or otherwise shown activity—conditions that families may not meet promptly after a death [2, 3]. The societal stakes are not only private. Researchers at the Oxford Internet Institute projected that the dead may outnumber the living on Facebook within decades, reframing digital legacy as a matter of collective memory as well as individual succession [4].

Against this empirical backdrop lie doctrinal fault lines. In the European Union, General Data Protection Regulation (GDPR) Recital 27 states that the Regulation does not apply to the personal data of deceased persons, leaving Member States to legislate tailored rules [5]. France's Data-Protection Law (Loi Informatique et Libertés [LIL], Article 85) does so by enabling binding post-mortem directives through which a person can define the fate of their data [6]. Germany's Federal Court of Justice (Bundesgerichtshof [BGH], 2018) held that a social-media user agreement is inheritable and passes to heirs, subject to privacy and memorialization constraints [7]. UK guidance

confirms that information about a deceased individual is not "personal data" under UK GDPR, while sectoral regimes (e.g., health records) may still govern particular contexts [8]. In the United States, most states have adopted the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), which enshrines an authority hierarchy that privileges provider "online tools," then wills or powers of attorney, then default statute, and draws a key distinction between communication content and catalog/metadata [9]. This framework attempts to reconcile fiduciary access with privacy norms for electronic communications.

These divergences motivate the three research questions this study pursues. First, what policy-ready definition and taxonomy of "digital legacy" best support governance across distinct categories? Second, how do comparative regimes perform in practice across four layers—nation-state law, industry standards and professional guidance, platform policies and tooling, and individual planning—and where do they succeed or fail? Third, how should China proceed under the Civil Code of the People's Republic of China (CCPRC) and adjacent regimes to effectuate user intent, protect post-mortem dignity and third-party privacy, and enable lawful succession at scale?

To answer these questions, the study adopts a comparative doctrinal and policy-analysis approach. It triangulates primary legal sources (statutes, regulations and case law, including RUFADAA, GDPR Recital 27 with Member-State implementations such as France's Article 85, and Germany's BGH decisions) with official platform documentation (e.g., Google's IAM and inactivity policy) and peer-reviewed research published between 2022 and 2025. Inclusion criteria privilege authoritative texts and provider-maintained materials. Comparative dimensions include the hierarchy of authority, scope of disclosure, evidence and verification standards, and privacy safeguards such as redaction for third-party communications. The analysis also attends to operational feasibility: since most digital legacy is hosted by private platforms, legal principles must be translated into auditable workflows, timelines and Application Programming Interfaces (APIs) if they are to work at scale.

The paper proceeds as follows. Section 2 introduces concept and status of digital legacy. Section 3 synthesizes international experience in managing digital legacy. Section 4 indicates China's challenges and suggested response under the CCPRC. Section 5 concludes by articulating a layered governance model.

2. Concept and Status of Digital Legacy

2.1. Definition and Taxonomy

Digital legacy denotes the bundle of accounts, data and digital assets that persist after a natural person's death. For governance and measurement, a functional taxonomy is more useful than a purely technical one because it maps directly onto legal interests and operational constraints. Three categories capture most post-mortem problems: direct-value digital assets (such as cryptocurrencies, tokenized items and in-game assets) in which patrimonial value and transferability are primary; derivative-value accounts (such as domain names, e-commerce stores and monetized channels) in which continuity, goodwill, and control dominate; and sentimental or cultural records (such as emails, photos, messages and cloud archives) in which dignity, memory, and third-party privacy must be balanced.

Comparative law and scholarship support this tripartite scheme. State statutes in the United States (e.g., RUFADAA) prioritize user intent expressed through provider "online tools" and distinguish communication content from catalog/metadata [9]. At the European level, GDPR Recital 27 excludes deceased persons from the Regulation, leaving Member States to legislate targeted post-mortem rules (e.g., France's post-mortem directives), while German case law treats social-media contracts as inheritable subject to privacy constraints [5-7]. These anchors collectively motivate a taxonomy that differentiates transferrable value, continuity-critical accounts and personality-laden materials. See Table 1 for a compact overview.

Table 1. Taxonomy of Digital Legacy

Category	Examples	Primary Interest	Governance Pain Points
Direct-value digital assets	Crypto wallets, Non-Fungible Tokens (NFTs) and in-game items	Transferability and valuation	Key access, licensing and custody
Derivative-value accounts	Domain names, stores and monetized channels	Continuity and goodwill	License vs. ownership; Intellectual Property (IP); branding
Sentimental/cultural records	Emails, photos, messages and archives	Memory, dignity and heritage	Post-mortem privacy and third-party consent

Note: Author's synthesis of a functional taxonomy informed by comparative law and peer-reviewed scholarship. Sources: [5-7, 9].

2.2. Status Quo

Globally, the scale and dispersion of digital footprints are substantial: social media penetration alone encompasses a majority of the world's population, and typical users engage with several platforms each month, implying that a decedent's data is commonly distributed across multiple services and jurisdictions. In parallel, provider housekeeping rules—such as inactivity-based deletion—affect what actually survives unless users have activated pre-death preference tools. Legal treatment also diverges. U.S. states have widely enacted RUFADAA's tiered authority model [9]. The European Union excludes deceased persons from GDPR and relies on Member-State legislation (for example, France's post-mortem directives) [5, 6]. Germany recognizes inheritance of platform contracts subject to privacy and memorialization limits [7]. The UK confirms that information about the deceased is not personal data under UK GDPR even as sector-specific regimes (notably health records) continue to apply [8]. These features together define a global baseline in which user intent, privacy to the living and operational feasibility must be reconciled.

China presents a particularly dense landscape. National statistics report very high levels of internet penetration and near-ubiquitous mobile access, with short-video and online-payment services reaching the overwhelming majority of netizens [10]. As a result, Chinese digital legacies typically include large volumes of communications and media, alongside finance-adjacent traces such as payment histories and account balances. Because these materials frequently co-implicate living third parties (for example, chat counterparties or faces in shared images), default privacy-preserving measures—in particular, redaction and scoped time windows—are central to any lawful disclosure workflow. At the same time, CCPRC's recognition of data and online virtual assets provides statutory footing for clarifying authority and effecting succession [11].

At the platform layer, major providers differ markedly in capabilities and default pathways. Apple supports Legacy Contacts, enabling designated persons to request scoped iCloud data with an access key and proof of death, while excluding decryption of Keychain and certain licensed media [12]. Google offers IAM for pre-death designation and enforces a two-year inactivity policy [2, 3]. Meta memorializes profiles with limited management by legacy contacts [13]. Microsoft generally relies on documentation-based processes and, for content access, legal orders [14]. Adoption and scope vary across services and products, which underscores the need for minimum capability baselines and interoperable, auditable workflows.

2.3. Related Scholarship

Recent researches reinforce the functional taxonomy above and clarify the normative stakes of post-mortem data. Morse and Birnhack advance a continuity principle, arguing that digital traces constitute an ongoing narrative that persists beyond death. They caution against asset-only approaches and support calibrated, context-sensitive disclosure [15]. Allen and Rothman and Nwabueze and White re-examine post-mortem privacy, proposing principled criteria for when and how privacy interests should extend after death and how they interact with heirs' claims and freedom of expression

[16, 17]. Building on earlier foundations (e.g., Kasket), Doyle and Brubaker synthesize Human-Computer Interaction (HCI) and socio-legal literatures to show persistent gaps in user planning and platform usability, while Kohl and Schäfer map the legal terrain where property, contract, and personality rights intersect in digital remains [18-21]. A growing thread interrogates downstream reuse: Nakagawa identifies ethical and regulatory risks in using the data of the deceased to train AI systems, pressing for purpose limitation, consent alignment and harm mitigation [22].

Across these strands, three themes converge. First, user intent captured before death—especially service-specific designations—should anchor governance but only alongside privacy protections for living third parties embedded in communications and shared media. Second, effective practice requires operational rails: evidence standards, redaction pipelines and auditable decision paths that platforms and courts can actually run. Third, cross-border divergence and heterogeneous platform tools motivate interoperability profiles that travel across jurisdictions. These findings motivate the cross-layer comparative analysis in Section 3 and the China-specific operational blueprint in Section 4.

3. International Experience in Managing Digital Legacy

3.1. Nation-State Law and Regulation

Table 2. Selected National Approaches

Jurisdiction	Status of Deceased's Data	Key Instrument/Case	Access Model	Notes
United States	Widely enacted state statutes	RUFADAA (Final Act with Comments)	Tiered: online tool, will/Power of Attorney (POA), default statutory rules	Distinguishes content vs. catalog/metadata.
EU (general)	GDPR excludes deceased	GDPR Recital 27	Member-state specific	National divergence by design.
Germany	Contracts inheritable	BGH Facebook (2018)	Heirs succeed to contract	Privacy and memorialization limits.
United Kingdom	Deceased not "personal data"	Information Commissioner's Office (ICO) guidance	Sectoral pathways	Health-records regimes apply.
Australia	Generally out of scope federally	Office of the Australian Information Commissioner (OAIC) guidance	Sectoral pathways	State health-information access rules.
New Zealand	Generally out of scope	Office of the Privacy Commissioner (OPC) guidance	Sectoral pathways	Health information pathways for deceased.

Note: High-level comparison of selected jurisdictions; table entries summarize the dominant legal instrument and practical access model. "Tiered: online tool, will/POA, default statutory rules" uses comma-separated phrasing per journal style. Sources: [5-9, 23, 24].

Across jurisdictions, statutory approaches have converged on the need to recognize user intent while safeguarding privacy and the integrity of electronic communications, yet they operationalize these aims differently. In the United States, the RUFADAA implements a three-tier authority hierarchy that privileges provider-specific "online tools" over testamentary instruments and default

statute, and it distinguishes content of communications (typically requiring explicit consent) from catalog/metadata (more readily disclosable) [9]. In the European Union, GDPR Recital 27 excludes the deceased from the Regulation's scope, prompting Member States to legislate tailored rules [5]. France authorizes binding post-mortem directives through its data-protection law [6]. Germany's Federal Court of Justice has held that social-media user contracts are inheritable, subject to privacy and memorialization constraints [7]. The United Kingdom confirms that information about the deceased is not "personal data" under UK GDPR, while sectoral regimes (notably health records) continue to govern disclosure in specific contexts [8]. Australia and New Zealand likewise place the deceased largely outside federal privacy acts but maintain sectoral pathways (especially in health) [23, 24]. Table 2 summarizes these models at a high level and highlights their practical implications for authority, scope and evidentiary burdens.

3.2. Industry Self-Regulation

Although few cross-industry standards address posthumous data directly, a set of widely adopted governance frameworks shapes how organizations implement retention, access controls and auditability that ultimately constrain post-mortem handling. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 (information security) and ISO/IEC 27701 (privacy information management) provide management-system requirements for authentication, logging, minimization and disclosure controls [25, 26]. In parallel, the U.S. National Institute of Standards and Technology (NIST) Privacy Framework and Special Publication (SP) 800-53 Rev.5 offer voluntary but detailed control catalogs that many platforms map to for risk management [27, 28]. Professional bodies add domain-specific guidance. The American Bar Association (ABA) and trusts-and-estates communities publish practical notes for embedding digital-asset authority into wills and powers of attorney [29]. The Law Society of England and Wales and Society of Trust and Estate Practitioners (STEP) curate practitioner guidance for evidencing authority and handling cryptographic keys [30, 31]. Health-record custodians (e.g., National Health Service [NHS] England) maintain procedures for lawful access to records of the deceased [32]. These instruments do not themselves create fiduciary access rights. Rather, they shape process, evidence and accountability baselines against which platform policies and court orders operate.

3.3. Platform Practices

Table 3. Comparative Platform Features

Provider	Pre-death designation tool	Memorialization	Data export to heirs	Message/content access	Notes
Apple	Legacy Contact (access key and proof of death)	N/A (account-level handling)	Scoped iCloud data; excludes Keychain/licensed content	No Keychain decryption; consent via Legacy Contact	Access key must be created before death.
Google	IAM (contacts, data selection and timer)	N/A (inactivity governs account state)	Pre-configured data sharing; account may be deleted after inactivity	Access per user's IAM configuration; otherwise limited	Two-year inactivity deletion policy.
Meta (Facebook/Instagram)	Legacy contact (Facebook)	Memorialized profile with limited management	Limited export; preservation over transfer	No full inbox disclosure; limited actions	Family or legacy contact triggers memorialization.
Microsoft	None (no native designation tool)	N/A	Case-by-case via documentation	Often requires legal process/court order	Support workflows emphasize formal proof.

Note: Coverage reflects publicly documented capabilities as of Aug 2025; features may vary by product and region. "N/A" denotes "not applicable." Sources: [2, 3, 12-14].

Large providers implement heterogeneous tools, reflecting different risk models and product scopes. Apple supports Legacy Contacts, enabling designated persons to request scoped iCloud data with an access key and proof of death, while explicitly excluding iCloud Keychain and certain licensed media from disclosure [12]. Google offers IAM, which lets users pre-select contacts, data types and inactivity timers [3]. It also enforces a two-year inactivity deletion policy across products [2]. Meta supports legacy contacts and memorialized accounts with limited management rights rather than full impersonation or inbox access [13]. Microsoft relies more heavily on documentation-based processes and, for communication content, legal orders [14]. Table 3 arrays these capabilities to clarify where pre-death designation, memorialization, export and content access are available and under what preconditions. Fig. 1 complements Table 3 by visualizing coverage differences across providers.

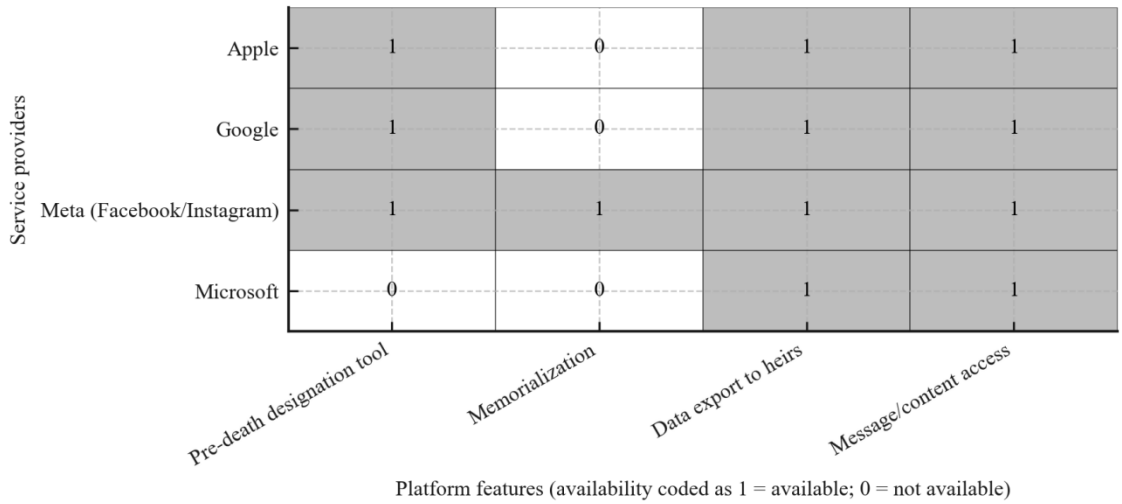

Figure 1. Platform Feature Coverage (illustrative). Matrix compiled by the author from official provider documentation; items shown are illustrative and may differ by product line, region, or account type. See Table 3 for textual detail

3.4. Individual Planning

International practice points to a pragmatic toolkit for individuals that travels well across jurisdictions. Users should enable provider-native tools where offered (Legacy Contact and IAM), incorporate digital-asset authority into wills and powers of attorney, and maintain an encrypted inventory of accounts and cryptographic keys with conditional release to executors. They should also classify sensitive communications and intimate media for deletion or restricted transfer and anticipate third-party privacy in shared threads and images through redaction-first defaults. In short, jurisdictions and platforms increasingly converge on the principle that clear, pre-death user intent—captured in service-specific tools and validated instruments—should guide post-mortem outcomes, provided that disclosures are narrowly tailored to minimize harm to the living. This logic prepares the ground for the comparative synthesis that follows and for its adaptation in the China-specific roadmap.

3.5. Synthesis of International Lessons

First, an authority hierarchy that privileges provider tools, then wills/POAs, then default statute yields predictable outcomes and reduces conflict with platform terms and cross-border variation. Second, even where general privacy law excludes the deceased, targeted national rules (e.g., France's directives) can restore user agency without undermining privacy limits. Third, framing social-media accounts as contracts (as in Germany) supports inheritance of control rights while rejecting impersonation and compelled speech. This lens also clarifies that property-like and personality-based interests must be balanced case by case. Fourth, platform tooling has matured sufficiently to justify minimum capability baselines—pre-death designation, memorialization, selective export, and

privacy-preserving content handling—implemented through auditable workflows. Persistent gaps remain in definitions, third-party privacy filtering, interoperability, and user uptake. These gaps directly inform the China-focused solutions.

4. China's Challenges and Suggested Response under the CCPRC

4.1. Challenges

4.1.1 Government

China already possesses two legal footholds for a comprehensive regime. Article 127 of CCPRC recognizes the protection of "data and online virtual assets," while Article 49 of the Personal Information Protection Law (PIPL) allows close relatives to exercise certain rights over a deceased person's personal information unless the decedent arranged otherwise [11, 33]. Read together, these provisions justify a dedicated pathway for post-mortem handling that both effectuates user intent and safeguards the privacy of the living. To move from principle to practice, lawmakers should clarify the scope of "digital legacy" with a policy-ready taxonomy, adopt a hierarchy of authority that gives primacy to service-specific "online tools" before wills and powers of attorney and then default rules, and specify an evidence and verification package that courts and providers can run at scale. Because many Chinese users' accounts involve cross-border storage or counterparties, the regime should also harmonize with cybersecurity and data-transfer rules so that disclosures to heirs are both narrowly tailored and lawful. A clear statutory baseline of concepts, authority, evidence and timelines would align private platform workflows with public law and reduce the need for ad hoc judicial invention.

4.1.2 Platforms

Any Chinese solution must begin where digital legacy actually resides: in a small number of high-penetration platforms across messaging, payments, short video and social media, e-commerce, and cloud. WeChat (including WeChat Pay) and QQ concentrate dense clusters of chats, contacts and transaction traces. Alipay aggregates balances and financial-adjacent records. Douyin, Kuaishou, Bilibili and Weibo retain videos, posts, comments and direct messages. Taobao/Tmall, JD.com and Pinduoduo record orders, invoices and wallet credits. Baidu Netdisk stores files and photos. National usage data indicate that short-video and online-payment services reach the overwhelming majority of netizens, which means typical legacies are high-volume, multi-service and finance-adjacent, often co-mingled with the data of living third parties. Although pre-death designation tools remain limited domestically, several providers already operate memorialization or deceased-account procedures and, on the financial side, permit inheritance of balances subject to documentation—practices that demonstrate feasibility even if they are still documentation-driven rather than API-standardized.

Therefore, a compliance-by-design approach would unify pre-death designation, post-death memorialization, selective export or deletion and redaction-first disclosure within a single, auditable module. To reduce friction for courts and executors, platforms should adopt standard evidence schemas (death certificate, identity, standing) and expose secure intake, verification, redaction and delivery APIs, backed by service-level targets and transparency dashboards. Because risks and product scopes differ across categories (messaging, media, finance and cloud), the regime should permit calibrated variants while insisting on a common minimum capability set aligned with the national-model and platform-feature baselines summarized in Table 2 and Table 3.

4.1.3 Individuals

While statutes and platform tools provide the legal and technical framework, outcomes ultimately depend on what people do before death. Individuals should enable provider-native controls wherever available, incorporate digital-asset authority into wills and powers of attorney, and maintain an encrypted inventory of critical accounts and cryptographic keys with conditional release to executors. They should also decide in advance which classes of content—especially intimate communications and shared images—should be deleted, restricted or transferred, thereby guiding relatives and

providers and reducing conflicts with third parties. Because PIPL recognizes close-relative rights, explicit instructions from the decedent help courts and platforms weigh those rights against the privacy of the living and the necessity of disclosure.

4.2. Suggested Response

4.2.1 Drafting Principles and Extract Articles

A workable statute or judicial interpretation can be organized around seven principles expressed in prose rather than checklists. The law should first define digital legacy and its sub-categories so that property-like assets, continuity-critical accounts and personality-centered materials receive appropriately differentiated treatment. It should then rank sources of authority—online tools, then testamentary instruments, then defaults—in order to minimize collisions between private terms and public law and to honor granular, service-specific consent. Next, it should set out a standard evidence package that platforms must accept and courts can recognize, including notarization or equivalent methods for proving death and kinship. Since many traces co-implicate the living, privacy-preserving disclosure must default to redaction, filtering and scoped time windows, with partial releases when full disclosure would foreseeably harm others. To make the system run, the statute should require a minimum platform toolkit—designation, memorialization, selective export and deletion—exposed via secure, logged APIs for courts and notaries. It should also impose timelines and auditability so requests do not linger and so actions are traceable, and provide proportional remedies and specialized review for hard cases. Headings for draft articles then follow naturally—Purpose and Scope, Definitions, Hierarchy of Authority, Evidence, Duties of Platforms, Minimum Disclosure, APIs and Interoperability, Timelines, Cross-Border Transfers, and Penalties—each coordinated with CCPRC and PIPL.

4.2.2 Implementation Blueprint for Chinese Platforms

Execution can proceed in phases without destabilizing existing user experiences. In the design phase (roughly months 0-3), platforms should form a cross-functional task force (legal, privacy, security, engineering, trust and safety), map account types and data sensitivities, and publish a human-readable policy that mirrors statutory language. During the build phase (months 3-9), they can stand up a modular Digital Legacy Center inside account settings with components for designation storage, case intake and triage, evidence verification, automated redaction (with human-in-the-loop for edge cases), export and delivery with hashes and manifests, and end-to-end audit logs. Minimal court/notary APIs and documentation can be piloted in parallel. The pilot phase (months 9-12) should test throughput and accuracy with selected courts and notaries while iterating on prompts that nudge users to set pre-death preferences. Finally, the scale phase (months over 12) can formalize service-level targets and publish transparency metrics (volumes, processing times, denial reasons, data categories), while participating in industry working groups to align interoperability and redaction profiles across providers. This staged build mirrors practices that already exist domestically and adapts international lessons to local constraints.

4.2.3 Judicial Balancing Test

When disputes arise, courts should articulate a proportionality-based test in narrative terms rather than rigid lists. The starting point is the clarity and recency of user intent—including platform designations and testamentary records. The court then weighs the nature and sensitivity of the requested data, the necessity and scope of disclosure (time windows, counterparties and services) and the availability of less intrusive alternatives. It also considers the foreseeable harm to living third parties and the public-interest dimensions of estate administration or cultural memory. Orders should always prescribe purpose limits, retention periods and security safeguards for recipients, authorize narrowly tailored disclosures—especially for communication content—and require logging that supports later review. This approach aligns with CCPRC's recognition of both property and personality interests and with PIPL's protective logic, while avoiding the paralysis that accompanies all-or-nothing access.

4.2.4 Risk and Cost–Benefit for Platforms

A clear account of platform risk clarifies why standardization is worth the engineering effort. The principal hazards are privacy leakage without robust redaction, impersonation or fraud without layered and auditable verification, and operational strain without partial automation and API-mediated workflows. There are also reputational risks if defaults are confusing or insensitive and compliance risks when disclosures intersect cross-border controls. Each of these is tractable: verification that combines document checks with device and behavioral signals, cryptographically verifiable submissions and redaction pipelines with human oversight can keep incidents rare; clear user experience with reversible choices and visible logs builds trust; and regionalized handling with lawful transfer mechanisms keeps data-flows compliant. On the benefit side, standardized legacy tooling promises lower litigation exposure, faster and fairer resolution for families, and measurable gains in public trust, which together justify making digital-legacy handling a normal part of the account life cycle rather than a crisis process triggered by loss.

5. Conclusion

This article addressed three questions: what policy-ready definition and taxonomy of digital legacy best support governance; how international approaches across national law, industry guidance, platform tooling and individual planning perform in practice; and what China-specific pathway under the CCPRC (with PIPL) can effectuate user intent, protect post-mortem dignity and third-party privacy, and enable lawful succession at scale. Using a comparative doctrinal and policy-analysis method that triangulated primary legal sources with official platform documentation and recent scholarship, the study defined a functional taxonomy—direct-value assets, derivative-value accounts and sentimental/cultural records—mapped global and China status, distilled portable lessons from comparative regimes and platform practices, and translated them into an operational roadmap for China.

Three conclusions follow. First, effective governance is layered: statutory baselines define terms, allocate authority, and set due-process guardrails; standards and professional guidance convert principles into organizational controls; platform tooling operationalizes those controls with usable interfaces and verifiable logs; user planning captures intent in advance. None suffices alone. Second, the authority hierarchy is pivotal. Prioritizing service-specific "online tools," then wills and powers of attorney, then default statute reduces collisions between private terms and public law and respects the granularity of user consent. Coupled with a principled distinction between communications content and catalog/metadata, this structure better protects the privacy of living third parties while enabling lawful access. Third, privacy-preserving disclosure is ethically required and technically feasible: redaction, filtering and scoped time windows—implemented through logged decision paths and narrowly tailored orders—allow courts and providers to balance dignity, succession, and others' rights without resorting to all-or-nothing access.

For China, moving from principle to routine practice entails codifying a clear taxonomy and authority hierarchy, requiring major platforms to ship a Digital Legacy module that supports pre-death designation, memorialization, selective export and deletion, and redaction-first disclosures, and exposing secure, auditable APIs for courts and notaries, with standardized evidence packets, service-level timelines and transparency dashboards.

Limitations include evolving platform policies, uneven translations of primary sources and gaps in empirical evidence on user and family preferences. Future work should maintain a versioned registry of platform capabilities, pilot standardized redaction and evidence-submission APIs in regulatory sandboxes, and run mixed-methods studies to calibrate defaults and consent flows. With these pieces in place, digital-legacy governance can become a dependable part of ordinary account life cycles rather than an emergency response triggered by loss.

References

[1] DataReportal and Kepios. Digital 2025: global statshot. Retrieved from: https://datareportal.com/reports/digital-2025-july-global-statshot, 2025. Accessed September 3, 2025.

[2] Google. Updating our inactive account policies (two-year inactivity deletion). Retrieved from: https://blog.google/technology/safety-security/updating-our-inactive-account-policies/, 2023. Accessed September 3, 2025.

[3] Google. About Inactive Account Manager. Retrieved from: https://support.google.com/accounts/answer/3036546, n.d. Accessed September 3, 2025.

[4] Öhman C J, Watson D. Are the dead taking over Facebook? A big data approach to the future of death online. Big Data & Society, 2019, 6 (1): 2053951719842540.

[5] European Union. General Data Protection Regulation (GDPR), Recital 27 (deceased persons out of scope). Retrieved from: https://gdpr-info.eu/recitals/no-27/, 2016. Accessed September 3, 2025.

[6] France. Loi Informatique et Libertés, Art. 85 (post-mortem directives) (consolidated text). Retrieved from: https://www.legifrance.gouv.fr/, n.d. Accessed September 3, 2025.

[7] Germany—Bundesgerichtshof (BGH). Facebook inheritance case, case no. III ZR 183/17. Retrieved from: https://www.loc.gov/item/global-legal-monitor/2018-09-07/germany-federal-court-of-justice-rules-digital-social-media-accounts-inheritable/, 2018. Accessed September 3, 2025.

[8] UK Information Commissioner's Office (ICO). What is personal data?. Retrieved from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/, n.d. Accessed September 3, 2025.

[9] Uniform Law Commission. Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA): final act with comments. Retrieved from: https://www.uniformlaws.org/viewdocument/final-act-with-comments-40, 2015. Accessed September 3, 2025.

[10] China Internet Network Information Center (CNNIC). The 55th statistical report on China's Internet development (Dec. 2024 data; English ed.). Retrieved from: https://www.cnnic.com.cn/IDR/ReportDownloads/202505/P020250514564119130448.pdf, 2025. Accessed September 3, 2025.

[11] Civil Code of the People's Republic of China, Art. 127 (data & online virtual assets). English translation. Retrieved from: https://www.chinalawtranslate.com/en/civilcode/, 2020. Accessed September 3, 2025.

[12] Apple. Legacy Contact-Digital Legacy. Retrieved from: https://support.apple.com/HT212360, 2024. Accessed September 3, 2025.

[13] Meta. Memorialization and legacy contacts. Retrieved from: https://www.facebook.com/help/1568013990080948, n.d. Accessed September 3, 2025.

[14] Microsoft. Accessing Outlook.com, OneDrive and other Microsoft services when someone has died. Retrieved from: https://support.microsoft.com/en-us/account-billing/accessing-outlook-com-onedrive-and-other-microsoft-services-when-someone-has-died-ebbd2860-917e-4b39-9913-212362da6b2f, n.d. Accessed September 3, 2025.

[15] Morse T, Birnhack M. The continuity principle of digital remains. New Media & Society, 2024, 26(9): 5240-5258.

[16] Allen A L, Rothman J E. Postmortem privacy. Michigan Law Review, 2024, 123 (2): 285.

[17] Nwabueze R N, White L. Privacy law and the dead—a reappraisal. Journal of Media Law, 2024, 16 (2): 253-277.

[18] Kasket E. Access to the digital self in life and death: privacy in the context of posthumously persistent Facebook profiles. SCRIPTed, 2013, 10 (1): 7-26.

[19] Doyle D T, Brubaker J R. Digital legacy: a systematic literature review. Proceedings of the ACM on Human-Computer Interaction, 2023, 7 (CSCW2): 268.

[20] Kohl U. What post-mortem privacy may teach us about privacy. Computer Law & Security Review, 2022, 46: 105717.

[21] Schäfer B. Post-mortem privacy and intergenerational trust. Computer Law & Security Review, 2023, 49: 105858.

[22] Nakagawa, H. Using deceased people's personal data in AI systems. Retrieved from: https://doi.org/10.1007/s00146-022-01549-1, 2024. Accessed September 3, 2025.

[23] Office of the Australian Information Commissioner (OAIC). What is personal information?. Retrieved from: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information, n.d. Accessed September 3, 2025.

[24] Office of the Privacy Commissioner (New Zealand). Health Information Privacy Code 2020. Retrieved from: https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Health-information-privacy-code-2020/Health-Information-Privacy-Code-2020-website-version.pdf, 2020. Accessed September 3, 2025.

[25] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—information security management systems—requirements. Retrieved from: https://www.iso.org/standard/27001, 2022. Accessed September 3, 2025.

[26] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27701:2019 security techniques—extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—requirements and guidelines. Retrieved from: https://www.iso.org/standard/71670.html, 2019. Accessed September 3, 2025.

[27] National Institute of Standards and Technology (NIST). Privacy Framework. Retrieved from: https://www.nist.gov/privacy-framework, 2020. Accessed September 3, 2025.

[28] National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53, Revision 5). Retrieved from: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final, 2020. Accessed September 3, 2025.

[29] American Bar Association (ABA), Real Property, Trust and Estate Law Section. How to protect digital assets in an estate plan. Retrieved from: https://www.americanbar.org/groups/real_property_trust_estate/resources/ereport/2025-winter/how-protect-digital-assets-estate-plan/, 2025. Accessed September 3, 2025.

[30] Law Society of England and Wales. Property (Digital Assets etc) Bill. Retrieved from: https://www.lawsociety.org.uk/en/topics/private-client/property-digital-assets-etc-bill, 2025. Accessed September 3, 2025.

[31] Society of Trust and Estate Practitioners (STEP). Digital assets: a call to action. Retrieved from: https://www.step.org/research-reports/digital-assets-call-action, 2021. Accessed September 3, 2025.

[32] NHS England (Transformation Directorate). Access to the health and care records of deceased people. Retrieved from: https://transform.england.nhs.uk/information-governance/guidance/access-to-the-health-and-care-records-of-deceased-people/, 2024. Accessed September 3, 2025.

[33] Personal Information Protection Law of the PRC (PIPL), Art. 49 (close relatives' rights for deceased). English translation. Retrieved from: https://www.chinalawtranslate.com/en/Personal-Information-Protection-Law/, 2021. Accessed September 3, 2025.