



THE LAST DIGITAL FOOTPRINT: RETHINKING THE RIGHT TO PRIVACY AND CONTROL OVER PERSONAL DATA IN THE DIGITAL AFTERLIFE AND RIGHTS IN THESE DIGITAL TIMES.

AUTHORS: Jasvir Singh Gyani, Priyanka Palani, Varsha Waghmare, Adv. Isha Pimpalikar.

ABSTRACT

Death only ends biological life and not necessarily the informational existence. In a world where people's lives are increasingly recorded and stored in digital spaces, the question of what happens to that information after death can no longer be treated as an optional issue. Yet privacy and data protection law have largely been developed around the living data subject.

This study, *The Last Digital Footprint: Rethinking the Right to Privacy and Control over Personal Data in the Digital Afterlife and Rights in These Digital Times*, examines this question through a qualitative, doctrinal, documentary, analytical and comparative legal approach. It begins with the theoretical foundations of post-mortem privacy, drawing on autonomy, dignity, informational self determination, informational identity and posthumous harm. Although these approaches explain the problem in different ways, they point towards a common concern: death, by itself, should not automatically bring every interest in a person's personal information to an end. At the same time, the study recognises that digital personal data, digital assets and digital identity are related but legally distinct.

The study then examines how law has attempted to respond to these questions through analysis of RUFADAA in the United States and the GDPR in the European Union shows that, despite important developments, existing frameworks do not fully address the problem of the digital afterlife. RUFADAA attempts to balance fiduciary access with the account holder's consent and confidentiality. The absence of a common international approach is particularly significant because digital information rarely remains within one jurisdiction: accounts, data, contractual



arrangements, heirs and platforms may all be subject to different legal systems. The research further shows that the issue is much broader than inheritance or access to a deceased person's account. Digital remains can contain information about people who are still alive. These digital remains may carry evidentiary, historical, cultural, emotional or legitimate inheritance value. This makes both automatic deletion and unrestricted preservation difficult to justify as universal solutions.

The role of digital platforms makes this problem even more difficult. Platforms increasingly determine, through account-management systems, memorialisation, deletion mechanisms and legacy tools, what happens to digital remains after death. Such mechanisms may give individuals some control over their digital afterlife, but voluntary tools cannot by themselves resolve conflicts between the deceased, heirs, living third parties and other legitimate interests. The problem is further complicated by the commercialisation of digital remains and by emerging generative technologies, which can transform the digital footprint from a record of a person's life into material capable of reproducing aspects of their voice, image, writing or behavioural characteristics. The digital afterlife therefore raises not only questions of preservation and access, but also questions of consent, dignity, authenticity and commercial exploitation.

The study therefore develops the basis for a legally grounded and adaptable framework which places post-mortem privacy and autonomy alongside the expressed wishes of the deceased, the rights of living third parties, legitimate succession and preservation interests, and clearer platform accountability. The study ultimately argues that death should not create a legal vacuum around a person's digital remains. The research argues for a move away from fragmented and largely reactive approaches towards a more coherent system of digital afterlife governance one that respects the autonomy and dignity of the deceased without disregarding the rights of the living, legitimate preservation interests or the accountability of the platforms that increasingly control what remains after we are gone.

INTRODUCTION



The rapid development and widespread use of digital technologies have profoundly changed the way people live, communicate, transact and store information about themselves. Social media platforms, electronic mail, cloud storage, online banking, digital health systems, mobile applications and other digital services generate constant records of the activities, relationships and identities of individuals. And perhaps these records will not, in fact, vanish with their creators. Instead, photographs, messages, profiles, digital accounts, personal information and other kinds of digital remains can survive, circulate and be repurposed long after the biological death of the individual. This has led to the concept of the digital afterlife, a general term for the persistence and management of a person's digital presence and remains after death (Harbinja, 2017; Öhman & Floridi, 2017).

The rise of the digital afterlife has posed a radical challenge to traditional Ideas of privacy, autonomy, dignity and personal identity. As people move through life, they are faced with more and more choices about what personal information to share, who can access it and how it can be used. But death raises questions about whether those choices should still matter legally and morally. The question is therefore not only what happens to information after a person dies but whether the deceased has any legitimate interest in controlling information that is produced during their lifetime. Buitelaar (2017) conceives this problem in terms of the concept of informational self-determination. He argues that control over personal information is closely connected to privacy and that the absence of a living individual should not automatically eliminate all interests in the protection of his or her informational identity. Similarly, Harbinja (2017) constructs postmortem privacy around autonomy and the individual's ability to control the fate of his or her digital identity and assets after death.

The problem is, however, complicated by the fact that digital personal data, digital identity And digital possessions are related but legally distinct concepts. Digital personal data may comprise correspondence, photographs, health information, financial information and other information relating to an identifiable individual. Digital resources can include accounts, digital files, cryptocurrency, domain names and other types of intangible property or value. Digital identity is a person's representation in digital environments; it consists of social-media profiles, photographs, usernames, online reputations and increasingly, technologically produced representations of personality. These categories raise different legal issues with regards to



privacy, property, succession, contractual rights and identity. Digital possessions do not always sit comfortably with traditional notions of inheritable property, as the same digital material can simultaneously carry economic, emotional and personal significance, as Mali and Prakash (2019) observe.

Consequently, the question of whether privacy and dignity can survive death has become an important topic of academic debate. Harbinja (2017) approaches the problem primarily from the angle of autonomy. Buitelaar (2017) connects the privacy of the deceased to dignity and informational self-determination. Another perspective is offered by Öhman and Floridi (2017) who stress the informational nature of human identity and argue that the commercial use of digital remains raises ethical questions that go beyond the life of the person. Recent work has broadened the concept, examining posthumous harm and the continuing moral significance of interests formed in life. In sum, these approaches offer competing but complementary explanations as to why the death of a person does not necessarily bring every interest in privacy to an immediate halt.

The theoretical debate has increasingly been supplemented by attempts to translate these ideas into legal mechanisms. One of the most important pieces of legislation in the United States to deal with fiduciary access to digital property in the event of death or incapacity is the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). The framework differentiates between kinds of digital information and tries to balance the interests of fiduciaries in administering an estate against the privacy expectations and intentions of the account holder. Its development also shows the difficulty of reconciling the interests of individuals, families, fiduciaries and technology companies. The American experience suggests that the acknowledgment of digital possessions after death does not necessarily lead to a straightforward inheritance model; issues of consent, confidentiality and the content of communications remain central to the legal framework.

The European Union has another model of regulation. The General Data Protection Regulation (GDPR) does not generally apply to the personal data of deceased persons. Recital 27 explicitly provides that the regulation of the personal data of deceased persons is a matter for the Member



States. Thus, although the GDPR provides for one of the most influential regimes for the protection of personal data during life, it does not create a comprehensive EU wide regime for post-mortem personal data. This creates an important distinction between the strength of data protection rights in life and the uncertain legal situation that may arise after death.

Internationally, the picture is far more fragmented outside of the United States and European Union. Comparative scholarship shows that jurisdictions have taken very different approaches to post-mortem personal information. Some jurisdictions provide limited recognition through inheritance, nomination or post-death directives, while others are silent. For example, India has introduced mechanisms relevant to the management of digital personal data and France has developed a framework that allows individuals to give instructions concerning the handling of their personal data after death. However, the approaches differ in scope and legal effect and do not establish a universally accepted model for post-mortem data governance.

The absence of an International standard is significant because digital information rarely remains in a single jurisdiction. A person's social media account can be managed by a company incorporated in one state, accessed by relatives in another and containing information on persons found in multiple jurisdictions. Information can be stored in several countries in cloud services and digital possessions can be governed at the same time by the terms of a contract, succession rules and data protection legislation. Hence, the death of a person may lead to a transnational legal problem as different legal systems give different consequences to the same digital information. The questions of jurisdiction, applicable law, contractual control and conflicting privacy interests, thus become inextricably linked to the question of post-mortem data protection.

Another important dimension concerns the role of technology platforms. Platforms can have a lot of power in determining how a person's digital remains are treated without comprehensive legislation. Others provide ways to memorialize, delete accounts, set up legacy contacts or manage inactive accounts. Such tools can give users a way to express their wishes about their digital afterlife, but how well they work depends a lot on how well users know about them, what the platforms allow and what the contracts say. Research has revealed a substantial gap



between people's stated desire to control their digital remains and their actual knowledge of, or use of, available digital-legacy mechanisms (Morse & Birnhack, 2022; Harbinja, McVey, & Edwards, 2024).

Also, platform control brings up the more general issue of the commodification of death and digital remains. Öhman and Floridi (2017) describe the emergence of a Digital Afterlife Industry, calling attention to the commercial interests involved in preserving, processing and potentially monetizing information concerning deceased persons. On a larger social level, the ever-growing digital profiles of dead users lead to questions about who benefits from the preservation of digital remains, and whether the interests of technology companies might be in conflict with the privacy and autonomy interests of users.

The problem is compounded by the fact that the digital remains of deceased persons may contain information about third parties who are alive. A private email may include more than one person; a photograph may identify surviving relatives; a social media conversation may include confidential information about another person; and a health record may reveal information about family members. Therefore, free access or automatic deletion cannot be a universally acceptable solution. In some instances preservation may safeguard family memory, historical record or legitimate inheritance interests. In other instances deletion may protect privacy and respect the wishes of the deceased. The challenge then becomes to determine when deletion, preservation, controlled access or transfer should prevail and which legal interests should prevail. The literature increasingly indicates that a calibrated approach is necessary and not a one size fits all rule.

The emergence of Artificial Intelligence' has added a new dimension to this problem. Advances in generative technologies are making it possible to reproduce aspects of a deceased person's voice, image, written work and behavioural characteristics. A digital footprint thus may no longer be a passive archive of an individual's past, but instead may be used to generate new content purporting to represent the deceased. This development raises issues of consent, personality rights, dignity, authenticity and commercial exploitation. It also challenges the



usual assumption of the relationship between death and identity, since technological representations may still interact with living persons long after the death of their creators.

These global developments are particularly important for countries in the Global South where the pace of digital adoption is rapid, but the post-mortem data governance may not have developed at the same pace. Nigeria is an important example. Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) provides for the privacy of the citizens, including their homes, correspondence, telephone conversations and telegraphic communications. Subsequently, Nigeria has enhanced its data protection regime through the Nigeria Data Protection Act 2023 which provides statutory protections for personal data and establishes the Nigeria Data Protection Commission as the main regulatory authority. However, the extent of these protections after an individual's death is still not well articulated. Nigeria's stance is emblematic of a wider global problem: the rapid development of digital identities and personal-data ecosystems has outpaced the development of clear rules governing what happens to those identities and data after death.

The significance of the Nigerian example lies not in it being the only jurisdiction with this problem, but in its demonstration of the intertwining of post-mortem privacy questions with constitutional rights, data protection, inheritance, family interests and emerging digital economies. It also emphasizes the importance of not assuming that regulatory solutions adopted in Europe or North America can be simply transplanted into other legal and social environments. Digital technology is inherently global and lends itself to comparative analysis, although questions of death, family, inheritance, privacy and identity may operate differently in different legal and cultural contexts.

Despite a growing body of scholarship, there remain substantial gaps in the international literature. In the existing literature extensive theoretical arguments have been developed concerning autonomy, dignity, informational self-determination and posthumous harm. Comparative studies have explored emerging legal responses and platform practices. But the question is how in practice the authority will be shared when the interests of the deceased, heirs, living third parties, platforms and legitimate preservation interests are in conflict. In



particular, the literature is less clear as to the precise obligations that digital platforms should bear when deletion, preservation and controlled transfer are competing possibilities.

Hence, this study explores “The Last Digital Footprint: Rethinking the Right to Privacy and Control Over Personal Data in the Digital Afterlife and Rights in These Digital Times” from a global and comparative perspective. It discusses the theoretical basis of post-mortem privacy, evaluates selected legal responses in different jurisdictions, analyses the role of digital platforms in the regulation of digital remains, and reflects on the implications of these developments for countries where dedicated post-mortem data-protection frameworks are still lacking. Particular attention is given to the competing interests of deceased persons, their heirs and personal representatives, living third parties, technology platforms, and legitimate preservation interests.

And in the end, the study wrestles with a question that existing privacy law was not designed to answer with certainty: when a person dies, does the right to control personal information die with that person? The answer cannot be that privacy ends with death; nor can it be that all digital information should forever be under the control of the dead. A more suitable approach necessitates a careful analysis of autonomy, dignity, succession, third-party rights, preservation interests and platform responsibility. With digital technologies allowing human identities and personal information to be extended beyond biological life, the legal boundaries of this digital afterlife have become an important question for contemporary privacy and data-protection law.

THEMATIC LITERATURE REVIEW & SYNTHESIS

Introduction

The question of what happens to a person’s privacy, dignity and digital identity after death has become increasingly important as individuals accumulate digital footprints that may substantially outlive them. Emails, social-media profiles, photographs, cloud accounts, health records and other digital remains can continue to exist, circulate, be copied, preserved or repurposed after biological death. It concerns what legal consequences should follow from that



survival, particularly where the wishes of the deceased, the interests of heirs, the privacy of living third parties, legitimate preservation interests and the practical control exercised by digital platforms do not point in the same direction.

The literature reviewed in this study is organised around four interconnected themes, namely, the theoretical foundations of post-mortem privacy through autonomy, dignity, informational self determination, informational identity and posthumous harm. The second considers how selected legal frameworks, particularly RUFADAA and the GDPR, attempt to address questions of access, control and erasure and where those frameworks remain limited. The third examines emerging approaches beyond the United States and European Union, with particular attention to India, France and Nigeria, while situating these examples within a broader but carefully framed comparative landscape. The fourth turns to digital platforms and the practical governance of digital remains, including questions of user choice, preservation, commercialisation and platform responsibility.

Digital personal data, digital assets and digital identity are related but not interchangeable concepts. Digital personal data may include correspondence, photographs, health information, financial information and other information relating to an identifiable person. Digital assets may include accounts, files, cryptocurrency, domain names and other intangible resources capable of having economic or succession value. Digital identity concerns a person's representation in digital environments, including profiles, usernames, photographs, online reputation and increasingly technologically generated representations. The legal consequences differ across these categories, engaging questions of privacy, property, succession, contractual rights and identity in different ways.

Theoretical Foundations: Privacy, Dignity and Personhood in the Digital Afterlife

The question of whether privacy continues after death has only recently received sustained attention in legal scholarship, but it lies beneath almost every claim concerning control over personal information after death. Without some theoretical account of why post-mortem interests matter, legal mechanisms concerning access, deletion or preservation risk becoming merely procedural rules without a clear normative basis.



Harbinja (2017) approaches post-mortem privacy primarily through autonomy and testamentary freedom. Her argument is that if the law already allows individuals to determine the disposition of property through wills, there is a plausible basis for extending a similar idea of control to aspects of digital identity. Buitelaar (2017), drawing on German constitutional thought, places greater emphasis on dignity and informational self-determination, connecting the ability to control personal information with the protection of the individual. These approaches overlap, but they are not identical: Harbinja's account is particularly concerned with continuing personal control through death, whereas Buitelaar's provides a broader constitutional and dignitary basis for informational interests.

Both approaches encounter what has been described as the "problem of the subject": if rights and interests attach to a person, how can those interests meaningfully continue once the person is dead? The objection matters because a post-mortem privacy claim must explain not only why the person's interests deserve protection, but what exactly is being protected and through whom that protection can be exercised.

Öhman and Floridi (2017) approach the issue differently by treating identity itself as informational. Their account suggests that a person can continue to be wronged through the exploitation or commercial use of their informational representation, even where the person is no longer conscious of the harm. Bak and Willems (2022) extend related concerns into health-data ethics, demonstrating that the ethical significance of information does not disappear merely because the data subject has died. Nwabueze and White (2026), drawing upon Boonin's theory of posthumous harm, provide a more recent attempt to address the conceptual difficulty directly. Their argument is that the relevant victim of posthumous harm need not be understood as a continuing conscious subject; rather, the interests of the person who existed while alive can be wronged after that person's death.

These accounts should not, however, be treated as establishing one uncontested theory. An autonomy-based account raises questions about how far individual control should extend where it affects others. A dignity-based account must address who is entitled to enforce dignity after



death. An informational-identity approach risks becoming exceptionally broad if every digital representation is treated as an extension of the person. A posthumous-harm account must still confront the question of how such harms can be translated into enforceable legal rights. The literature therefore provides substantial support for taking post-mortem interests seriously, while leaving open the precise scope and legal form of those interests.

What emerges from this literature is consequently more nuanced than the simple proposition that “privacy survives death”. The stronger proposition is that death does not, by itself, necessarily extinguish every legal or ethical interest attached to a person’s personal information, identity or dignity. The remaining questions concern the scope of those interests, the persons or institutions who may enforce them, and the circumstances in which they should give way to competing interests.

Existing Legal Responses: RUFADAA and the GDPR

The theoretical case for post-mortem privacy has been accompanied by attempts to translate aspects of that interest into legal mechanisms. Among the principal legal responses examined in this literature are the United States’ Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) and the European Union’s General Data Protection Regulation (GDPR). Rather than describing these as definitively “the two most developed responses globally”, it is more accurate to treat them as important and comparatively developed examples of different regulatory approaches to digital access and personal-data governance.

RUFADAA is significant because it addresses fiduciary access to digital assets and attempts to reconcile estate administration with the privacy expectations and intentions of the account holder. Its development also demonstrates that recognising digital assets within succession law does not produce an automatic inheritance model. According to Lopez (2016), an earlier and broader approach that would have granted fiduciaries more extensive default access encountered resistance, with the eventual framework adopting a more differentiated approach. Fiduciaries may obtain a catalogue of communications, while access to the actual content of communications is more restricted and may depend upon the account holder’s prior consent or judicial authorisation.



This compromise reveals an important feature of digital succession: access to an asset is not necessarily equivalent to access to the information contained within that asset. A person may have a legitimate succession claim over an account or digital asset without thereby acquiring an unlimited entitlement to read every private communication associated with it. Allen and Rothman's (2024) broader analysis also indicates that post-mortem protection in the United States remains uneven, with certain protections appearing more clearly where the deceased's identity retains commercial significance.

The GDPR presents a different legal problem. It provides extensive rights concerning the processing of personal data of living persons, including access, rectification and erasure. Yet its relationship with deceased persons is fundamentally limited. The literature notes that the GDPR generally does not apply to the personal data of deceased persons and leaves the regulation of such data to Member States. Article 17 therefore cannot be treated as a freestanding EU-wide postmortem privacy right. Its relevance here lies partly in showing the strength of a living person's right to erasure and, at the same time, the limits of attempting to extrapolate that framework directly into the post-mortem context.

The question is also one of implementation. Politou, Alepis and Patsakis (2018) identify technical difficulties surrounding erasure, particularly where information is reproduced across backups, immutable systems or other technical infrastructures. Ruohonen and Hjerpe's (2022) analysis of 294 enforcement decisions adds a different insight: erasure was a secondary basis for enforcement action, while variation in the severity of fines appeared to depend more strongly on the country of enforcement and the year than on the particular provision breached. This finding should not be used to claim that the study proves erasure itself to be ineffective; rather, it demonstrates that the practical enforcement of data-protection law cannot be understood solely by looking at the existence of an erasure right on paper.

The comparison between RUFADAA and the GDPR is therefore useful precisely because the two regimes expose different limitations. RUFADAA demonstrates the difficulty of balancing fiduciary access, consent and confidentiality. The GDPR demonstrates the limits of relying on



a life-centred data-protection framework when the individual is deceased. Neither, in the form examined here, provides a comprehensive answer to questions of long-term digital identity, postmortem privacy, AI-generated replicas, third-party privacy and the broader allocation of authority among heirs, platforms and other interested parties.

Emerging and Global South Frameworks: Jurisdictional and Conceptual Gaps

The limitations become more visible when the analysis moves beyond the principal US and EU examples. The comparative material does not support an absolute claim that there is a “near-total absence” of post-mortem protection everywhere outside those jurisdictions. What it does support is a more cautious conclusion: deliberate post-mortem treatment remains uneven across jurisdictions, and there is no common international model for governing digital remains. The selected jurisdictions therefore demonstrate fragmentation rather than complete legal silence.

India, France and Nigeria are particularly instructive because they demonstrate different ways in which post-mortem questions intersect with privacy, data protection, succession, property, constitutional rights and contractual relationships. India’s Digital Personal Data Protection Act 2023 provides an important statutory framework for digital personal data, including consent, data principal rights and obligations imposed on data fiduciaries. The Act nevertheless does not create a comprehensive standalone regime for post-mortem digital privacy or fully resolve the status of digital identity and digital inheritance after death. Its nomination mechanism is therefore significant, but does not by itself resolve all questions concerning control over accounts, communications or digital remains after the death of the data principal.

France presents a more explicit post-death model. Its Digital Republic framework permits individuals to leave directives concerning the handling of personal data after death, including retention, deletion and disclosure, and provides mechanisms involving trusted persons and heirs in appropriate circumstances. Yet the French approach does not amount to a complete solution. Questions surrounding AI repurposing of deceased persons’ data, cross-border enforcement and conflicts between heirs, platforms and broader public interests remain insufficiently resolved.



The Nigerian example is significant for a different reason. Nigeria combines constitutional privacy protections with the Nigeria Data Protection Act 2023, yet the extent to which those protections continue after death remains insufficiently articulated. This illustrates a wider problem in jurisdictions experiencing rapid digital adoption: the development of digital identity and personal data ecosystems may outpace the development of rules governing what happens to those identities and data after death.

The wider legislative mapping undertaken in the study covers the European Union, United Kingdom, India, Brazil, Japan, South Korea, Canada, Australia, Germany, Singapore, New Zealand, China, Indonesia, Malaysia, Thailand, South Africa, Nigeria and Kenya. The table is useful as a map of general data-protection architecture: covering matters such as personal-data protection, consent, data-subject rights, security, organisational obligations and cross-border transfers but it should not be read as evidence that each jurisdiction has a dedicated post-mortem privacy regime. The prose analysis should therefore concentrate on the jurisdictions for which the literature and primary legal material support a substantive post-mortem discussion.

This distinction also helps refine the classification problem identified by Mali and Prakash (2019). Digital assets are difficult to fit into traditional succession categories because a single item may have economic, emotional, personal and legal significance simultaneously. A succession regime may tell us who inherits a digital asset, but it does not necessarily tell us who should be allowed to access every item of personal information connected to it.

The broader picture therefore reflects two connected problems rather than a claim of universal legal silence. First, there is doctrinal uncertainty about how digital personal data, digital assets and digital identity should be classified and governed after death. Secondly, the selected empirical literature points towards institutional and public uncertainty about using the mechanisms that do exist. These findings are important, but they should be attributed to the populations and contexts actually studied.



What Do People Actually Want? Digital-Legacy Planning and the Implementation Gap

The empirical material adds an important dimension to the doctrinal literature because it moves the discussion from what the law provides to what individuals say they want, and then asks how far those preferences are actually translated into arrangements.

Harbinja, Morse and Edwards' study of 1,766 UK residents provides useful evidence of this tension. Approximately four in five respondents indicated that they wanted a known relative to have access to their digital remains on relevant platforms after death, while around 19–24% preferred that no one should receive access. Among those who favoured access, approximately seven in ten wanted access to all content on the relevant platform, and the spouse was the most commonly identified person for personal accounts. At the same time, approximately 62.6% were classified by the study as experiencing an “inverted posthumous privacy paradox”: they expressed a preference for post-mortem access but had not made arrangements that would actually enable it.

These findings are important, but they should not be presented as a universal behavioural pattern. The figures arise from a particular UK sample and study design. Their value lies in illustrating a contradiction: people may have fairly definite views about what should happen to their digital remains while failing to convert those views into practical arrangements.

More recent evidence provides a useful, although not directly comparable, point of reference. Meißner and Mahaj (2026), in a study of 396 participants, found that 69.3% of those who had not yet planned their digital legacy intended to manage it in the future, while 59.7% said that their online presence or digital legacy should be deleted after death. Yet only 20.6% had created a digital-legacy will, either completely or partially, and only 22.8% had formulated instructions concerning what should happen to their digital accounts. The study further reports that 65.1% had at least partially thought about their digital legacy, while 50% had at least partially informed themselves about it.



A 2025 representative survey by Bitkom Research provides a further perspective from Germany. Among 1,003 German residents aged 16 and above, including 917 internet users, 32% of internet users reported having made at least some arrangements concerning their digital estate after death, with 16% having completely arranged the matter and 16% partially arranged it. Twenty-two per cent planned to make arrangements in future, while 43% indicated that they would not or did not want to make arrangements. The same survey reported that 60% did not want anyone to have access to their digital content after death, whereas 40% wanted their social-media profiles to remain. Yet only 3% had actually configured an online service or social network to place their profile in a memorial state, and among those who had made some arrangements, only 15% had made provisions specifically for social-media accounts.

The earlier Bitkom survey from 2017 reported that 72% of German Internet users welcomed statutory regulation for digital estates comparable with inheritance law. The two Bitkom data points should be kept separate rather than treated as an eight-year trend, since the question wording, survey context and methodology may differ. The 2017 figure is useful as evidence of public support for legal regulation; the 2025 figures are more useful for showing continued uncertainty and limited practical implementation.

Taken together, the available empirical literature does not show that people want one uniform model for the digital afterlife. Some want access granted to relatives, some want deletion, some want preservation and some want restrictions. What appears more consistently is an implementation problem: preferences concerning digital legacies may be stronger and clearer than the practical arrangements made to give effect to them.

Platform Power and Commercialisation: The Limits of Voluntary Digital-Legacy Governance

Once digital remains are held primarily through private technological infrastructure, the question of platform governance becomes a legal question rather than merely a technological one. Unlike physical property, digital remains are often stored, authenticated, accessed and controlled through systems owned or operated by private companies. A family member seeking access to the digital remains of a deceased person may therefore depend not only upon



succession law but also upon contractual terms, authentication requirements, platform policies and technical architecture.

Harbinja (2017) identifies technological tools for managing digital remains, including Google's Inactive Account Manager. More recent work by Morse and Birnhack (2022) and Harbinja, Morse and Edwards (2024) indicates a continuing gap between people's stated desire to exercise some degree of control over their digital remains and their awareness or use of the tools available for doing so.

The UK survey material gives this point greater specificity: only 28% of the 1,766 adults surveyed had heard of platform tools such as Facebook Legacy Contact, Apple Legacy Contact and Google Inactive Account Manager. Actual activation was reported at approximately 8% for Facebook, 5% for Google and 7% for Apple, while around 72% were unaware of these mechanisms. These figures should be used as evidence about that UK sample, not as evidence of global platform behaviour.

The legal significance of platform governance follows from this practical dependence. Platforms often determine whether an account can be memorialised, deleted, transferred or accessed. Their role therefore places them between the preferences of the deceased and the claims of those who survive them. Where the law provides no clear rule, a platform's contractual policy may effectively become the rule in practice. The important legal question is consequently how much authority over a person's digital afterlife should be left to private contractual arrangements.

The problem changes further when preservation occurs at scale. Öhman and Watson (2019) consider the prospect of billions of deceased user profiles and shift the debate from individual preference to the broader social consequences of preserving digital remains. Preservation may have genuine cultural and historical value, but the commercial interests of platforms may also shape what is retained and how it is used. Kohl (2022) adds another complication by emphasising that post-mortem information frequently concerns living third parties. These



observations support a conflict analysis, but they do not by themselves establish that commercial interests always determine platform behaviour.

The emergence of generative technologies adds a newer dimension. The digital footprint may no longer remain merely a record of the deceased person's past. Technologies can reproduce aspects of a person's voice, image, writing and behavioural characteristics, raising questions of consent, authenticity, dignity, personality rights and commercial exploitation. The legal issue therefore moves from preserving an existing record to creating new representations from data associated with a person who can no longer consent.

The literature therefore supports the relevance of platform governance to post-mortem privacy because platforms possess the practical capacity to determine what happens to digital remains. It does not, however, justify the broader claim that all platforms behave alike or that commercial interests necessarily determine every post-mortem decision. The stronger conclusion is narrower: private platform rules occupy a significant practical position in a regulatory field where public law remains fragmented, making questions of transparency, accountability and minimum legal standards difficult to avoid.

CONFLICTING RIGHTS IN THE DIGITAL AFTERLIFE

The literature increasingly demonstrates that post-mortem digital privacy is not a single-right problem. It is a problem of competing interests.

Deceased Person's Privacy Versus Family's Interest In Access

A deceased person may have wished emails, photographs or social-media content to remain private, while family members may seek access for grief, memorialisation, family history or estate administration. The conflict becomes particularly acute where access to the deceased's account exposes information belonging to people who are still alive.



The European Data Protection Board has described the relational nature of this problem in direct terms: “A deceased person’s communications may contain personal data belonging to living third parties”. The point is legally important because family access can simultaneously become disclosure of information concerning someone who remains alive.

Privacy Versus Inheritance And Property Interests

Digital accounts may contain financial assets, documents, intellectual property, photographs and other material of economic or personal significance. France demonstrates that succession interests can be recognised without treating every item contained within an account as automatically accessible to heirs.

Deceased Person’s Wishes Versus Heirs’ Wishes

Where the deceased has left express instructions, those directions provide a stronger basis for determining post-mortem treatment. The more difficult situation arises where no clear instructions exist, because heirs may have legitimate interests while the law may provide no clear basis for resolving competing claims.

Privacy Versus Access To Communications Involving Others

A deceased person’s communications are rarely “their data” alone. An email may contain another person’s private correspondence, sensitive family information or material involving third parties. Access decisions must therefore account for the privacy interests embedded within the communication itself.

Security During Life Versus Access After Death

The security measures encouraged during a person’s lifetime- strong passwords, encryption, multifactor authentication and restricted access may become obstacles for lawful post-mortem administration. The same security architecture that protects autonomy while a person is alive can make lawful access difficult when no arrangements were made beforehand.



Digital remains exist within systems largely designed, owned and controlled by private companies. Unlike physical property, access to digital remains often depends upon the platform's technical architecture, terms of service, authentication requirements and internal policies. Families seeking access may therefore depend upon the cooperation of platforms even where they may have a legitimate succession or familial interest in the material. Where the law provides no clear answer, the platform's contractual and technical rules may, in practice, determine whether digital remains can be accessed, preserved, memorialised or deleted. This makes platform governance a legal issue rather than merely a technological one, because private terms and technical design can effectively determine the extent to which post-mortem interests can be exercised.

The tension becomes more complicated where Information concerning a deceased person has a legitimate public, journalistic or historical value. In such cases, the interests protected by privacy cannot simply be treated as overriding the public's interest in receiving information. At the same time, the fact that information about a person's death may legitimately be published does not necessarily mean that the same information can be freely repurposed for commercial gain. A recent French parliamentary question illustrates this distinction. Published in the French Senate on 4 June 2026, Senator Bruno Belin drew attention to the use of publicly available death data by private funeral and media platforms to create tribute or obituary pages, including through forms of indirect monetisation. The question specifically distinguishes publication connected with the freedom to inform from the subsequent economic exploitation of post-mortem information, and asks whether the existing legal framework provides adequate protection against non-consensual commercialisation of grief.

These conflicts demonstrate why a simple hierarchy in which one party always wins is difficult to sustain. They also explain why the phrase "calibrated approach" needs substantive content. Calibration cannot simply mean "balance the interests". It should involve identifiable considerations, including the nature and sensitivity of the information, the deceased person's expressed wishes, the identity and purpose of the person seeking access, the impact on living third parties, the existence of a legitimate preservation or public-interest justification, and the consequences of disclosure or deletion.



LITERATURE SYNTHESIS AND RESEARCH GAP

Taken across the themes, the literature reveals a clear progression. The first stage asks whether post-mortem interests are legally and ethically intelligible at all. Theoretical scholarship increasingly answers that question in the affirmative, although it differs on precisely why and in what form those interests survive. The second stage asks how existing law handles access, succession and erasure. Here the picture is less settled: legal systems offer partial mechanisms, but these mechanisms were not generally designed as comprehensive post-mortem regimes. The third stage concerns how individuals and institutions actually use those mechanisms, where recent empirical work points towards a gap between preferences and implementation. The fourth concerns who should carry legal responsibility when individual preference, family claims, thirdparty privacy, preservation and platform control conflict.

Agreement therefore begins to break down once the literature moves from recognition to implementation. It would be too broad to say that all scholars agree that privacy simply survives death. The stronger and more supportable proposition is that a substantial body of scholarship rejects the idea that death automatically makes privacy, dignity or informational interests legally irrelevant. The harder question is how those interests should be structured once other rights are brought into the analysis.

Likewise, the literature does not justify treating RUFADAA, the GDPR, French directives or Indian nomination mechanisms as stages in one linear model of legal development. They respond to different legal problems and operate within different constitutional, statutory and institutional settings. Their comparative value lies in the recurring questions they expose: consent, fiduciary access, confidentiality, succession, deletion, contractual control and the difficulty of translating individual preferences into enforceable rules.

The empirical literature adds a further complication. Available studies suggest that people often care about their digital legacy and may hold strong preferences concerning access, preservation or deletion, yet many have not translated those preferences into formal arrangements. The UK, German and other survey findings should therefore be treated as contextual evidence rather than as proof of a universal behavioural pattern.



At the same time, the literature reveals an asymmetry between individual responsibility and institutional responsibility. Individuals are increasingly encouraged to make wills, nominate contacts or configure digital-legacy tools, yet the legal system does not always establish what platforms must do where no such arrangements exist, where instructions are ambiguous, or where an otherwise legitimate request threatens the privacy of a living third party.

This brings the review to the central issue of platform duty. The selected literature suggests that platform governance occupies a critical practical space, but the precise legal obligations of platforms remain less clearly developed than the broader theoretical debate about post-mortem privacy. The claim should therefore be framed carefully: the present review identifies a gap within the selected literature concerning the operationalisation of platform obligations, rather than asserting that no scholarship anywhere has addressed the issue.

The study therefore Identifies three connected gaps. First, there remains a gap between the theoretical recognition of post-mortem interests and the practical legal consequences attached to that recognition. Secondly, the selected empirical literature provides useful evidence concerning preferences and digital-legacy planning, but there remains limited evidence concerning what happens when those preferences are actually invoked after death, particularly across jurisdictions. Thirdly, there is a more specifically legal gap concerning authority and platform responsibility when the wishes of the deceased, the interests of heirs, the privacy of living third parties, legitimate preservation interests and platform policies conflict.

The contribution of the present study lies primarily In addressing this third problem through doctrinal and comparative analysis. Rather than treating post-mortem privacy as a question of whether the rights of the deceased simply continue unchanged, the study considers how different interests should be organised when digital information survives its creator. The objective is to develop principles for a legally grounded and adaptable framework addressing deletion, preservation, controlled access and transfer while taking account of autonomy, succession, third party privacy, legitimate preservation interests and platform accountability.



The literature therefore leads to a more precise question than the starting question of whether the dead can have privacy: when a person's digital footprint survives their death, who should have the authority to decide what happens to it, on what legal basis, subject to whose competing rights, and with what obligations imposed upon the platform that controls it?

METHODOLOGY

1. Research Design

This study adopts a qualitative doctrinal, documentary, analytical, and international legal research design. The doctrinal approach is used to examine existing legislation, judicial decisions, legal principles, and regulatory frameworks governing post-mortem privacy and control over personal data. The documentary approach extends the analysis to international legal instruments, scholarly literature, and digital-platform policies. An analytical approach is adopted to identify inconsistencies, regulatory gaps, and practical difficulties within existing legal responses. The international dimension enables the study to examine legal approaches across jurisdictions and identify principles capable of informing a coherent and replicable framework. The design is therefore appropriate because the study seeks not only to determine the current state of law but also to develop a policy framework addressing the deletion, transfer, preservation, and protection of digital footprints after death.

2. Nature of Research

The research is qualitative, doctrinal, analytical, and policy-oriented in nature. It relies primarily on textual and legal evidence rather than numerical measurement or statistical analysis. The study examines how legal rules and institutional practices address posthumous digital privacy, digital identity, personal data, and digital assets. It further evaluates the extent to which existing mechanisms protect individual autonomy while balancing the interests of heirs, living third parties, digital platforms, and legitimate preservation interests. The policy-oriented dimension enables the study to formulate a legally grounded and adaptable framework for post-mortem digital data governance.



3. Sample & its Technique

As the study does not involve human respondents, its sample consists of purposively selected legal and documentary materials. These include relevant legislation, judicial decisions, international legal instruments, regulatory materials, academic literature, and digital-platform policies. Materials will be selected according to their relevance to posthumous privacy, digital identity, control and access to personal data, deletion, transfer or inheritance, preservation, anonymity, and platform responsibility. Relevant materials from different jurisdictions will be examined to identify recurring legal principles, weaknesses, and approaches that may contribute to a framework capable of broader implementation.

4. Data Collection Tool

The study employs documentary and secondary data collection. Primary legal materials, including legislation, judicial decisions, and relevant legal instruments, will be identified through authoritative legal and institutional sources. Secondary materials, including scholarly articles, books, reports, and legal commentary, will provide theoretical and analytical support. Digital platform policies will also be examined to determine how platforms currently address account management, data access, deletion, memorialisation, and post-mortem control. The materials collected will be organised thematically according to the research questions and the principal analytical dimensions of the study.

5. Variables Used

Given the qualitative legal nature of the study, conventional independent and dependent statistical variables are not applied. Instead, the study examines key legal concepts and analytical dimensions, including post-mortem privacy, digital identity, digital footprint, personal-data control, deletion, transfer or inheritance, anonymity, heirs' rights, third-party privacy, platform obligations, and legitimate preservation interests. These concepts will be analysed to determine how existing frameworks balance competing rights and interests and where further legal regulation may be required.



6. Ethical Considerations

The study does not involve direct human participants or the collection of private participant data. Ethical considerations therefore focus primarily on the accurate and responsible use of legal and scholarly materials. All sources will be appropriately acknowledged and cited, and legal authorities will be represented accurately. Where sensitive information concerning deceased individuals is discussed, unnecessary disclosure of personal information will be avoided, and relevant privacy and data-protection principles will be respected.

7. Limitations

The study may be limited by the fragmented and rapidly evolving nature of posthumous digital privacy law. Differences in legal terminology, regulatory structures, and platform policies across jurisdictions may make the development of a universally applicable framework challenging. Reliance on publicly available legal and documentary materials may also limit access to confidential platform practices and internal decision-making. Furthermore, the study is primarily doctrinal and documentary, accordingly, the proposed framework should be understood as a legally and analytically grounded model that may require adaptation to specific national legal systems.

DATA ANALYSIS

LEGAL BASIS

UK Study

In a study titled “Digital remains and post-mortem privacy in the UK: what do users want?” conducted a survey May 2023 of 1,766 UK residents, aged between 18-90 and it specifically examined people’s wishes concerning their digital accounts and data after their death. The study showed that 4 in every 5 respondents wanted to grant someone access to their digital remains on various platforms after death, that number approximately comes to ≈ 1413 respondents out of a total 1766 who wished for their data to be managed by a known relative



after their death, an overwhelming majority. In the same data it also highlighted that only about 19% to 24% said they wanted to grant access to no one. Out of the approximately 80% who wanted to grant access, about 7 in every 10 wanted the person to have access to all the content on the relevant platform. The most common person chosen for personal accounts was a spouse.

The study also identified an “Inverted Posthumous Privacy Paradox” wherein, although majority participants desired for post mortem data access and control, many of those respondents had not taken practical steps, or made arrangements such that would be necessary to enable and implement those preferences, approximately 62.6% were classified within this paradox. This shed light on an implementation gap, where majority failed to act in preference of their wishes and desires.

[Study Methodology: Cross-sectional online survey conducted in May, 2023. Quota sampling to be nationally representative of UK adults. Quotas based on age, gender, and region. Sample size- 1766 participants, ages 18 to 90.]

German Study 1

In a separate study by Meißner, A. & Mahaj, D. (2026), “The digital legacy in end-of-life care: unspectacular and meaningless, or not enough recognized?” they surveyed 396 participants and found that 69.3% of the respondents who had not yet planned their digital legacy said they planned to manage it in the future. In the same study, 59.7% said their online presence/ digital legacy should be deleted after their death. Yet only 20.6% had created a digital-legacy will, either completely or partially, an action gap that becomes defining of the “inverted posthumous privacy paradox”. Only 22.8% had formulated instructions about what should happen to their digital accounts after death. While only 65.1% had at least partially thought about their own digital legacy. And 50% had at least partially informed themselves about digital legacy.

The following figures are drawn from a 2026 survey of 396 participants. Because the available study information does not establish that the study information is nationally representative, the



figures are interpreted as evidence of respondent attitudes and behaviour rather than as estimates of the wider population.

Criteria	Data in %
Respondents who had not yet planned their digital legacy said they planned to manage it in the future.	69.3
Respondents who said their online presence/digital legacy should be deleted after their death.	59.7
Respondents who created a digital-legacy will, either completely or partially.	20.6
Respondents who had formulated instructions about what should happen to their digital accounts after death.	22.8
Respondents who had at least partially thought about their own digital legacy	65.1
Respondents who had at least partially informed themselves about digital legacy.	50

*Source: “The digital legacy in end-of-life care: unspectacular and meaningless, or not enough recognized?” by Meißner, A. & Mahaj, D. (2026)

[Study Methodology: Cross-sectional nationwide online survey conducted in Germany; convenience sampling via palliative and hospice organizations; 396 participants, healthcare professionals and volunteers in palliative care; age groups of 20-29, 30-39, 40-49, 50-59, and 60+] The above table shows the opinions of individuals on the subject of Digital Privacy Rights after their death, it tabulates how about 65.1% had at least partially thought about digital legacy, while only 20.6% has created a digital will, and only 22.8% formulated instructions about what should happen to their digital accounts after death.



A 2025 survey in Germany by Bitkom Research Representatives surveying 1003 German residents aged 16+, including 917 internet users, showed that 32% of German internet users had made at least some arrangements for what should happen to their digital estate after death, 16% had completely arranged it and 16% had partially arranged it. 22% of respondents planned to arrange their digital estate in the future, and 43% of respondents said they would not or did not want to make arrangements. The same study also found that 60% said they explicitly did not want anyone to have access to their digital content after their death. While 40% wanted their social media profiles to remain after their death. Yet only 3% had actually configured an online service/ social network to put their profile into a memorial state after death. Among people who had made some arrangements, only 15% had made provisions specifically for social media accounts.

[Study Methodology: A nationally representative online survey conducted in the year 2025; sample size- 1003 German residents; aged 16 and above; including 917 internet users]

This data shows how deeply people cared about their digital privacy after death and had strong opinions about how their data should be treated after their death, whether they made arrangements to ensure those wishes or not.

German Study 3

Bitkom had an earlier 2017 representative survey where 72% of German internet users said they would welcome a statutory/legal regulation for digital estates comparable to inheritance law. An overwhelming statistical majority calling for legal frameworks about Posthumous Digital Privacy Rights.

[Study Methodology: Nationally representative survey; conducted of 1013 German residents; aged 14 and above; including 842 internet users]

This study strongly indicates the public demand for statutory regulation of digital estates, since it may help bridge the gap between desire to control post mortem digital data and actively taking steps to ensure them. A statutory regulation may encourage and inform individuals to



actively seek to protect their digital privacy not only when they are living persons but also when they are not.

LEGAL FRAMEWORKS

Even though digital privacy and data protection legislation has become widespread and common globally, these frameworks predominantly regulate the collection, processing and protection of personal data primarily during an individual's lifetime. The extent to which they recognise and protect an individual's digital privacy after death remains considerably less developed. Some of such global legislation is mentioned below.

Jurisdictions	Legislation	What it regulates
European Union	General Data Protection Regulation (GDPR)	• Personal data protection • Consent and lawful processing • Access, correction and erasure rights • Data security and breach obligations • Cross border data transfers
United Kingdom	UK GDPR + Data Protection Act, 2018	• Personal data protection • Individual data rights • Consent/lawful processing • Data security and breach notification • Regulation of organisations processing personal data
India	Digital Personal Data Protection Act, 2023 (DPDP Act)	• Digital personal data protection • Consent and lawful processing • Data principal rights • Duties of data fiduciaries • Children's data • Data security and breaches



Brazil	Lei Geral de Proteção de Dados (LGPD)	• Personal-data protection • Consent and lawful processing • Data-subject rights • Sensitive personal data • Data-security obligations • Regulatory enforcement
Japan	Act on the Protection of Personal Information (APPI)	• Personal information protection • Individual rights • Business obligations • Sensitive information • Data transfers • Regulatory oversight
South Korea	Personal Information Protection Act (PIPA)	• Strong personal data protection • Consent and processing • Data subject rights • Sensitive information • Security/breach obligations • Cross border data transfers
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	• Private sector personal information • Consent • Individual access/correction • Accountability • Security safeguards • Disclosure/use restrictions
Australia	Privacy Act, 1988	• Personal information protection • Australian Privacy Principles • Collection/use/disclosure controls • Access and correction • Data security • Data breach notification



Germany	Federal Data Protection Act (BDSG) + GDPR	• Personal data protection • Employee data • Public sector processing • Individual rights • Data security obligations • Enforcement
Singapore	Personal Data Protection Act (PDPA)	• Consent • Collection/use/disclosure of personal data • Individual access/correction • Security • Data breach notification • Cross border transfers
New Zealand	Privacy Act, 2020	• Personal information protection • Collection/use/disclosure rules • Access and correction • Privacy principals • Data breach notification • Cross border disclosure
China	Personal Information Protection Law (PIPL)	• Personal information protection • Consent • Individual rights • Sensitive personal information • Data security requirements • Cross border transfers
Indonesia	Law No. 27 of 2022 on Personal Data Protection	• Personal data protection • Consent processing • Data subject rights • Sensitive data • Security and breaches • Cross border transfers



Malaysia	Personal Data Protection Act 2010	• Personal data processing • Consent • Data subject rights • Security • Disclosure/use restrictions • Cross border transfers
Thailand	Personal Data Protection Act 2019 (PDPA)	• Personal data protection • Consent • Data subject rights • Sensitive data • Security/breach obligations • International transfers
South Africa	Protection Of Personal Information Act (POPIA)	• Personal information protection • Lawful processing • Individual rights • Security • Data breaches • Regulatory enforcement
Nigeria	Nigeria Data Protection Act 2023	• Personal data protection • Consent and lawful processing • Data subject rights • Security • Breach obligations • Regulatory enforcement
Kenya	Data Protection Act 2019	• Personal data protection • Consent • Data subject rights • Data security requirements • Cross border transfers • Regulatory oversight

*Source: Author's compilation based Jurisdictional Parliamentary Laws in place.



[The table provides a broad mapping of data-protection frameworks across selected jurisdictions. It is not intended to constitute an equivalent doctrinal analysis of each jurisdiction. Detailed analysis is subsequently limited to jurisdictions that provide particularly relevant mechanisms for post mortem data governance, namely the European Union, India, the United States, and France.]

Jurisdictions examined above have laws that regulate Protection of personal data, rights of the data subject, consent, data security, obligations of organizations, and cross-border data transfers and enforcement, but either do not expressly regulate Digital Privacy Rights of the deceased or do not apply to deceased persons.

Digital Personal Data Protection Act, 2023 (DPDP Act, India) has regulated the protection of living individuals' digital personal data, consent for processing, rights to access, correction and erasure, duties for data fiduciaries including security safeguards and breach notification, rules for children's data, and cross-border data transfers, but it does not create a standalone posthumous digital privacy right, nor does it not specify control of a deceased person's digital identity, and also does not comprehensively address digital inheritance. While it allows nominating another person to exercise rights after death, it doesn't detail how that covers digital accounts or long-term data control.

Although the DPDP Act introduces an important nomination mechanism, it remains centered on living data protection and does not establish a comprehensive solution for posthumous digital privacy.

General Data Protection Regulation, Regulation 2016/679 has made laws enabling lawful processing of personal data, data subject rights including access, rectification, and Article 17's right to erasure ("right to be forgotten"), principles like purpose limitation and data minimization. What it does not adequately address is posthumous digital privacy, because GDPR generally does not apply to deceased persons. It leaves that to member state legislation.



Both the DPDP Act and GDPR fail to address a standalone right to posthumous digital privacy, control of digital identity after death, management of social media and online accounts after death, digital inheritance or assets succession, balancing the deceased's privacy with family interests and platform policies, or detailed rules for AI use of posthumous data. These shared gaps across major legal systems support the need for a dedicated framework.

USA's RUFADAA addresses digital assets and fiduciary access rules, estate and trust administration, user consent and online tool directives, and duties for custodians when responding to lawful requests, but does not regulate upon a standalone posthumous digital privacy right or a long-term digital identity control. And like GDPR and the DPDP Act, does not address social media account management after death or AI-generated digital replicas or a detailed framework balancing heirs, platforms, and the deceased. While all mentioned legislation is robust in life, it leaves significant gaps after death, underscoring the need for a dedicated legal framework for posthumous digital privacy.

France's Digital Republic Act (Loi pour une République numérique, 2016) has made laws upon giving individuals the right to leave directives about their data after death, covering retention, deletion, or disclosure instructions, with general or specific directives, appointment of a trusted person to carry out those instructions, limited rights for heirs to access data needed for estate administration, and obligations for online service providers to inform users about post-mortem data handling. What it has not addressed is the regulation of AI repurposing deceased data, cross border enforcement, or a unified regime for digital Inheritance or disputes between heirs and platforms. So, compared to the GDPR and India's DPDP Act, France goes further by allowing posthumous directives, yet even France doesn't fully regulate AI uses of the deceased, cross-border issues, or a comprehensive balancing of heirs, platforms, and public interests.

Framework	What it contributes	Limitations
GDPR	Erasure and data protection principles	Deceased persons generally outside the GDPR scope
DPDP	Nomination mechanism	Doesn't create post-mortem digital rights



RUFADAA	Fiduciary access to digital assets	Primarily an estate access framework rather than privacy regime
DRA	Explicit post-death directives	Still leaves important issues such as AI/cross-border questions

The above table represents a concise analysis of the discussed frameworks' unique contributions and main limitations.

CONFLICTING RIGHTS

1. Deceased Person's Privacy vs. Family's Right To Access

The deceased may have wanted their messages, photographs, emails, or social-media data to remain private. While at the same time, family members may want access for grief, memorialisation, family history.

We should directly prioritise the deceased person's wishes and any claim saying otherwise should be overlooked, digital privacy does not end at death of the person but at the erasure of the data.

2. Privacy vs. Inheritance/ Property Rights.

Digital accounts can contain data with inheritance, commercial or financial value, such as digital assets, documents, photographs, intellectual property. France recognises this issue, and therefore allows for its citizens to appoint heirs to distribute assets, including digital estate, and family memories.

All digital assets should listed and distributed alike as compared to how physical assets are distributed, and in case of undistributed or non listing of said assets, they will legally distributed as like physical assets, in case of a dispute.



3. Deceased Person's Wishes vs. Heirs' Wishes

While France allows a person to leave directives about what should happen to one's personal data after death, allow them to appoint an heir to implement such wishes, But in the absence of such expressed directives, heirs may exercise certain rights themselves, other major laws on Digital Privacy Rights do not address this issue.

In case there is an heir but no clear directives, the heir should be restricted from using the deceased's personal information, communication, and photographs, media for commercial incentives, since it directly breaches the deceased's right to privacy.

4. Privacy vs. Access To Communications Involving Other People

A deceased person's messages aren't necessarily only their data. An email from a deceased person may contain:

- a) The deceased's personal information;
- b) Another person's private correspondence;
- c) Sensitive information about family members;
- d) Third-party photographs or messages.

The EDPB warns that exchanges belonging to a deceased person can also contain data concerning living third parties, therefore accessing such communication exchanges exposes confidential information surrounding the living individuals, therefore granting access to heirs to such data may compromise the privacy of a living individual.

Access to communication streams including private and confidential of living third parties should not be allowed even if one party allows for access to such communication, since the stream of communication and string of media is linked with privacy rights of two distinct persons, therefore access consent should be given by both these individuals, either implied or express.

5. Security During Life vs. Access After Death

While most privacy and security insist on people to use strong passwords, encryption tools, multiple factor authentication, password managers, limited account access, etc., but the same



mechanisms make it difficult for surviving family members from accessing data after the person's death, with the absence of such passwords.

All accounts of deceased persons should be unlocked after it is proven that the now deceased has implied for someone to access said accounts and a verified proof of such deceased person is provided, protecting information while living should not translate to cursing the information to be locked away after death, with no one being able to access it, accessing such accounts should be made simpler and easier.

6. Family Interests vs. Platform Interests And Contractual Rules

Most platform control much of the system that hold digital remains of a person, while the physical possessions do not harbour the same problem, digital remains of a person is held in lines of code, built of system that companies own themselves, therefore families of the deceased must enjoy the cooperation of such platforms and companies to access the data remains of their loved ones.

No company's rules should ultimately hinder a family from accessing digital data that belongs to the family's deceased relative, for that data, if consented to be accessed, might be the final memory or existing artifact that resonates with the elements of the since deceased, digital data rights, and rights to allocate such data are sacred once the deciding person can no longer alter the made decision, that consent to access their data becomes their final form of affection, one from beyond the grave.

7. Privacy vs. Public Interest/Freedom Of Information

This becomes particularly difficult when the information surround a public figure or holds journalistic value. In a parliamentary exchange, published on 4 June 2026 Senator Bruno Belin asked the French Government to clarify the legal and ethical dilemma. Senator drew important distinctions between freedom of information and commercial exploitation, and how publishing the fact of someone's death may be legitimate, but the information it into a commercially monetized article or data piece without the family's prior consent lead to complex legal questions that need strong affirmations to what the law clearly states and allows with information related to public interest.



Publicly accessible information, that today is just a click or search away, is protected under international conventions of copyright law, and may be used under provisions of education, information or other statutes under “fair use”, however all private information, that isn’t readily accessible to the vast public should be protected under privacy rights, unless consented to be used by an individual by the now deceased or their appointed heir.

Platform Obligations

In a previous cited study, it showed only 28% of 1,766 UK adults surveyed had heard of platform tools such as Facebook Legacy Contact, Apple Legacy Contact, and Google Inactive Account Manager. Actual activation was just 8% for Facebook, 5% for Google, and 7% for Apple. 72% of respondents were unaware of Facebook, Google, and Apple’s tools for managing digital accounts after death.

While there exist platform support systems, most individuals are unaware of them, and even less have actually activated or implemented them on their personal data, this may have occurred due to lack of comprehensive policies that ensures data would be protected until it is either erased or passed on, or because no broader legal framework enforces such policies, making it unpopular for its practical inefficiency.

Social platforms that harbour digital data policies should protect, and allow for seem-less reallocation or smooth erasure through policies that regulate post mortem digital data, and encourage, endorse more and more people start taking steps to ensure their private data is protected or in safe hands after their passing.

CONCLUSION

The discussion in this study determines that death does not necessarily bring the legal significance of a person’s digital identity to an end. A person’s e-mails, social-media profiles, photographs, health records, cloud accounts, communications and other forms of digital remains may continue to exist long after death. What remains unresolved is not simply whether such information continues to exist, but who should control it, who may access it, when it



should be deleted, when it should be preserved, and what should happen when the interests of the deceased come into conflict with the interests of living persons, heirs, platforms and legitimate preservation interests.

Theories and posthumous harm approach the issue from different directions, but they broadly point towards the obvious conclusion that death, by itself, should not automatically extinguish every interest connected with a person's personal information. At the same time, this does not mean that privacy after death can simply be treated as an exact continuation of privacy during life. The more difficult question is which interests should continue, who should be able to enforce them, and how far they should extend where other legitimate interests are involved.

When examining RUFADAA and the GDPR demonstrate that attempts have already been made to address aspects of digital access, control and erasure, but they do not provide a complete answer to the problem of the digital afterlife. The American approach reflects a compromise between fiduciary access and the deceased person's prior consent, while the European framework leaves important questions concerning deceased persons unresolved and faces practical difficulties in giving effect to erasure.

The problem becomes even more apparent when the analysis moves beyond the United States and European Union. There is no common international model for post-mortem data protection. Different jurisdictions approach personal data, digital assets and digital identity differently, and even jurisdictions that have begun to recognise some form of post-mortem protection have not yet developed a fully settled framework. This is particularly important because digital assets cannot always be treated as ordinary inheritable property. The same digital information may carry economic, personal, emotional and legal significance at the same time. A succession based approach, therefore, may determine who can inherit something without necessarily answering whether that person should have unrestricted access to the information contained within it.



The study also shows that the problem cannot be reduced to a simple conflict between the deceased and their heirs. Post-mortem data often contains information relating to other living persons. Communications, photographs, health information and social-media content may involve third parties whose privacy interests continue even after the original account holder has died. At the same time, certain digital remains may have legitimate evidentiary, historical, cultural or social value. This makes both automatic deletion and unrestricted preservation problematic. The literature instead points towards a more calibrated approach in which deletion, preservation or controlled transfer depends upon the deceased person's expressed wishes, the interests of living third parties and the existence of a legitimate reason for preservation.

This is also where the role of digital platforms becomes difficult to ignore. Platforms already exercise considerable practical control over what happens to digital accounts after death through mechanisms dealing with account management, deletion, memorialisation and access. Yet voluntary digital-legacy tools cannot, by themselves, constitute a comprehensive legal regime. The literature shows a continuing gap between the importance users attach to controlling their digital remains and the actual awareness or use of the mechanisms available to them. More importantly, existing scholarship has not sufficiently answered the question of what platforms are legally required to do when deletion, preservation and controlled transfer come into conflict.

The central gap, therefore, is not merely the absence of legislation. It is the absence of a sufficiently coherent framework for allocating rights, responsibilities and decision-making authority after death. The literature has developed the theoretical justification for post-mortem privacy considerably further than it has developed the practical obligations that should follow from recognising that interest. The unresolved issue is how law should respond when the wishes of the deceased, the interests of heirs, the privacy of living third parties, preservation interests and the practical control exercised by platforms point in different directions.

The study therefore supports the need for a legally grounded and adaptable framework for postmortem digital data governance. Such a framework should not proceed on the assumption



that every digital footprint must be deleted upon death, nor should it treat death as an automatic transfer of unrestricted control to heirs or platforms. Instead, it should distinguish between different forms and uses of digital information and determine the appropriate response according to the circumstances. The expressed wishes of the deceased should have significant weight, but they cannot necessarily operate in isolation where the information concerns living third parties or where a genuine and legitimate preservation interest exists.

In this context, platform responsibility becomes particularly important. Where platforms have the practical ability to delete, preserve, restrict or transfer digital information, their role cannot be left entirely to voluntary policies. A coherent framework should provide clearer standards concerning the circumstances in which platforms must act, the evidence required before access or deletion is permitted, the protection of third-party information, and the possibility of review where competing claims arise. The objective should not be to impose unrestricted liability upon platforms, but to ensure that decisions concerning a person's digital remains are not governed solely by private contractual arrangements or inconsistent platform practices.

At the same time, the conclusions of this study must remain within the limits of its research design. The study is qualitative, doctrinal, documentary, analytical and policy-oriented. It relies on legislation, judicial decisions, international legal instruments, scholarly literature, regulatory materials and digital-platform policies to identify legal principles, inconsistencies, regulatory gaps and practical difficulties. It does not empirically measure the frequency or effectiveness of postmortem data requests. Accordingly, the proposed framework should be understood as a legally and analytically grounded model rather than as an empirically validated universal solution. This distinction is important because the strength of the study lies in its doctrinal and comparative analysis, and the final claims should remain consistent with that methodology.

Ultimately, the digital afterlife exposes a mismatch between the posthumous existence of personal information and a legal framework that had traditionally been working to regulate the living data subject. The individual may die, but the digital footprint does not necessarily disappear with them. It may remain accessible, transferable, commercially valuable,



historically significant or capable of affecting others. The law therefore needs to move beyond the binary assumption that personal data must either remain completely private or become freely accessible after death.

The more appropriate approach is a calibrated framework which recognises post-mortem privacy and autonomy while also protecting the rights of living third parties, legitimate succession interests and genuine preservation needs. It should provide clearer obligations for platforms, distinguish between digital personal data, digital assets and digital identity, and establish safeguards for deletion, preservation and controlled transfer rather than treating any one of these outcomes as universally appropriate.

The central conclusion, therefore, is not that privacy simply continues after death in exactly the same form. It is that death should not create a legal vacuum in relation to a person's digital remains. The persistence of digital identity requires the persistence of legal questions around control, access, protection and responsibility. What is required is not perpetual control by the deceased, unrestricted access by heirs, or complete discretion for platforms, but a principled system capable of deciding, in each relevant context, whose interests are affected, what protection is justified, and what legal response is proportionate. Such a framework would move post-mortem digital privacy from a largely fragmented and reactive area of law towards a more coherent system of digital afterlife governance.

The more appropriate approach is a calibrated framework which recognises post-mortem privacy and autonomy while also protecting the rights of living third parties, legitimate succession interests and genuine preservation needs. It should provide clearer obligations for platforms, distinguish between digital personal data, digital assets and digital identity, and establish safeguards for deletion, preservation and controlled transfer rather than treating any one of these outcomes as universally appropriate.

The central conclusion, therefore, is not that privacy simply continues after death in exactly the same form. It is that death should not create a legal vacuum in relation to a person's digital



remains. The persistence of digital identity requires the persistence of legal questions around control, access, protection and responsibility. What is required is not perpetual control by the deceased, unrestricted access by heirs, or complete discretion for platforms, but a principled system capable of deciding, in each relevant context, whose interests are affected, what protection is justified, and what legal response is proportionate. Such a framework would move post-mortem digital privacy from a largely fragmented and reactive area of law towards a more coherent system of digital afterlife governance.

POLICY RECOMMENDATIONS

The research shows that post-mortem digital governance is no longer simply a question of what should happen to a deceased person's account. It is a question of how individual wishes can be made legally effective, how competing interests can be handled, and how responsibility can be allocated between individuals, heirs, platforms and public authorities. The following five recommendations translate those findings into a practical framework. The aim is not to transfer ownership of citizens' digital lives to the State, but to create a secure and legally recognised mechanism through which individuals can exercise meaningful control over what remains after death.

1. Establish a Government-Backed Digital Legacy Portal

Jurisdictions should establish a secure public digital legacy portal, administered by an appropriate Ministry or Department of Digital Affairs or equivalent authority. The portal should serve as a central point where citizens can record and manage instructions for their digital footprint, without creating a single government repository containing the underlying contents of all their accounts.

Registration should take place through a government-approved digital identity mechanism. Once verified, the individual should be able to create a digital legacy profile and identify the relevant email accounts, social-media accounts, cloud services, websites and other digital identities to which their instructions apply. The portal should principally function as a verified instruction and authorisation layer: it should record the individual's directions and



communicate them securely to the relevant platform or custodian rather than routinely storing the underlying content itself.

All information held within the portal should be encrypted. Government officials should have no routine right to inspect the contents merely because the system is government-backed. Access to the contents should require a specific statutory basis and, where appropriate, independent or judicial authorisation. The State may verify and administer the system without acquiring a general right to read the private digital lives recorded within it.

2. Give Citizens Express, Account-Level Choices

For each linked account or digital profile, the individual should be able to select one of three principal outcomes: (i) complete erasure; (ii) memorialisation; or (iii) transfer to a designated heir or authorised person. These choices should be made separately for each account because a person's wishes may differ across platforms.

The framework should also permit a person choosing memorialisation or transfer to give more specific instructions about particular categories of information. For example, an individual may wish an account to pass to a designated person while requiring private chats or direct messages to be deleted. In this way, control over an account would not automatically become unrestricted access to every item of information contained within it.

Where no express direction has been recorded for a particular account, the law should provide a statutory default process rather than leaving the outcome entirely to platform terms of service. Silence should not automatically be treated as consent to disclosure.

3. Separate Digital Assets from Personal Digital Data

Digital assets should be dealt with separately from ordinary personal digital data. The same account may contain material of economic or succession value as well as intensely private



information, and a succession right over an asset should not automatically confer unrestricted access to all personal information stored within that account.

Citizens should therefore be able to identify relevant digital assets through the digital legacy portal and designate the person entitled to receive them. Where a valid designation exists, that direction should be given effect subject to the applicable succession law. Where no designation exists, the asset should devolve according to the relevant statutory succession rules—for example, by reference to the applicable class of heirs under Indian succession law where that is the governing regime.

This approach avoids creating a parallel and disconnected law of digital inheritance. Instead, the proposed system would make digital assets identifiable and administratively accessible within the existing succession process while keeping the treatment of personal communications and other private data subject to separate safeguards.

4. Introduce a 180-Day Preservation Period and Tiered Erasure

Irreversible deletion should not ordinarily begin immediately upon notification of death. A statutory preservation period of 180 days should apply before final erasure, particularly because digital remains may have evidentiary, financial, legal or investigative significance and because disputes concerning access, inheritance or third-party privacy may arise only after death.

The 180-day period should not amount to an indefinite right of retention. It should operate as a limited cooling-off and preservation period during which lawful objections, preservation requests and appeals can be considered. A competent authority or court should also be able to direct continued preservation where a genuine legal or evidentiary need is established.

After the applicable period, erasure should proceed in three tiers:



- Tier I — Private communications and behavioural data: chats, direct messages, email content where deletion has been instructed, search history, watch history and comparable records of private activity.
- Tier II — Posted and shared material: photographs, videos, public or shared profile content, wishlists, likes and comparable user-generated or user-curated material.
- Tier III — Residual technical data: cache data, residual account information, technical identifiers, metadata where legally appropriate, and other miscellaneous data capable of lawful technical erasure.

The tiered model gives practical meaning to the study's calibrated approach. Not every digital trace carries the same privacy significance, and not every category should necessarily be treated in the same manner or at the same stage.

5. Protect Shared Data, Living Third Parties and Provide an Appeal Mechanism

Deletion or transfer should never be treated as affecting only the deceased. Digital remains may contain information belonging to living third parties, including private correspondence, photographs, family information and other material that continues to attract privacy or confidentiality interests. The framework should therefore require platforms to distinguish between the deceased person's account or copy of information and information in which another living person has an independent legal interest.

Where material is jointly held, jointly accessible or otherwise independently controlled by another person, deletion of the deceased person's account should not automatically destroy the other person's lawful access. Where disclosure to an heir would expose sensitive information concerning a living third party, the information should be capable of being restricted, redacted or withheld where justified.



The framework should also establish a straightforward appeal and review mechanism. Heirs, designated representatives and affected living third parties should be able to challenge an access, preservation or deletion decision within a defined period. Platforms should provide reasons for decisions and maintain an auditable record of significant actions.

This prevents the digital afterlife from becoming a system in which the first claimant automatically wins. It also creates accountability where platform terms, technical architecture and competing legal interests collide.

Operational rule: verified and unverified profiles

The five recommendations above should operate through two forms of registration. A verified profile would be linked to a government-approved identity and would become operational upon legally recognised confirmation of death, such as the issuance and verification of a death certificate. An unverified profile could still receive the same baseline encryption and privacy protection, but the individual would be required to select a future activation date for the chosen post-mortem instructions. The distinction prevents an unverified instruction from being treated as evidence that death has already occurred while still allowing individuals who do not use the government identity system to make meaningful arrangements.

Why these five recommendations?

Together, the five recommendations form a single system rather than five unrelated reforms. The first creates the trusted infrastructure; the second gives the individual meaningful choices; the third prevents succession rights from being confused with unrestricted access to personal information; the fourth prevents premature destruction while making erasure practicable; and the fifth protects the interests of living persons while creating accountability and review. The result is a framework that seeks to translate post-mortem wishes into enforceable action without placing a deceased person's digital life entirely in the hands of heirs, platforms or the State.

REFERENCES



Meißner, A., & Mahaj, D. (2026). The digital legacy in end-of-life care: unspectacular and meaningless, or not enough recognized? An online survey on the attitudes and personal experiences of professionals and volunteers. *BMC Palliative Care*, 25, 189. <https://doi.org/10.1186/s12904-026-02212-y>

Bitkom. (2025, 17 October). Digitales Erbe: Was passiert mit Online-Zugängen nach dem Tod? Bitkom e.V. <https://www.bitkom.org/Presse/Presseinformation/Digitales-Erbe-Online-Zugaengenach-Tod>

Bitkom. (2017, August 10). Die wenigsten regeln ihren digitalen Nachlass [Few people make arrangements for their digital estate]. Bitkom e.V.: <https://www.bitkom.org/Presse/Presseinformation/Die-wenigsten-regeln-ihren-digitalenNachlass.html>

Harbinja, E., Morse, T., & Edwards, L. (2025). Digital remains and post-mortem privacy in the UK: What do users want? *International Review of Law, Computers & Technology*, 40(1), 4–27. <https://doi.org/10.1080/13600869.2025.2506164>

European Data Protection Board (EDPB). (2022). Guidelines 01/2022 on data subject rights – Right of access (Version 2.0, adopted 28 March 2023). European Data Protection Board. https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-ofaccess_0.pdf

Belin, B. (2026, 4 June). Clarification des modalités d’encadrement juridique d’utilisation des données post-mortem [Written question No. 08990]. Sénat, Journal officiel. <https://www.senat.fr/questions/base/2026/qSEQ260608990.html>



Harbinja, E., Morse, T., & Edwards, L. (2025). Digital remains and post-mortem privacy in the UK: What do users want? *International Review of Law, Computers & Technology*, 40(1), 4–27. <https://doi.org/10.1080/13600869.2025.2506164>

Allen, A. L., & Rothman, J. E. (2024). Postmortem privacy. *Michigan Law Review*, 123(2), 285. <https://michiganlawreview.org/journal/postmortem-privacy/>

Bak, M. A. R., & Willems, D. L. (2022). Contextual exceptionalism after death: An information ethics approach to post-mortem privacy in health data research. *Science and Engineering Ethics*, 28(4), Article 32. <https://doi.org/10.1007/s11948-022-00387-0>

Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, 19(2), 129–142. <https://doi.org/10.1007/s10676-017-9421-9>

Government of India. (2023). *The Digital Personal Data Protection Act, 2023*. India Code.

Holt, J., Nicholson, J., & Smeddinck, J. D. (2021). From personal data to digital legacy: Exploring conflicts in the sharing, security and privacy of post-mortem data. *Proceedings of the Web Conference 2021*, 2745–2756. <https://doi.org/10.1145/3442381.3450030>

Kohl, U. (2022). What post-mortem privacy may teach us about privacy. *Computer Law & Security Review*, 47, Article 105737. <https://doi.org/10.1016/j.clsr.2022.105737>

Allen, A. L., & Rothman, J. E. (2024). Postmortem privacy. *Michigan Law Review*, 123(2), 285. <https://michiganlawreview.org/journal/postmortem-privacy/>



Bak, M. A. R., & Willems, D. L. (2022). Contextual exceptionalism after death: An information ethics approach to post-mortem privacy in health data research. *Science and Engineering Ethics*, 28(4), Article 32. <https://doi.org/10.1007/s11948-022-00387-0>

Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, 19(2), 129–142. <https://doi.org/10.1007/s10676-017-9421-9>

Government of India. (2023). The Digital Personal Data Protection Act, 2023. India Code.

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>

Harbinja, E., McVey, M., & Edwards, L. (2024). Post-mortem privacy and digital legacy: A qualitative enquiry. *SCRIPTed*, 21(4), 4–39.

Harbinja, E., Morse, T., & Edwards, L. (2024). Digital remains and post-mortem privacy in the UK: What do users want? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4813651>

Holt, J., Nicholson, J., & Smeddinck, J. D. (2021). From personal data to digital legacy: Exploring conflicts in the sharing, security and privacy of post-mortem data. *Proceedings of the Web Conference 2021*, 2745–2756. <https://doi.org/10.1145/3442381.3450030>

Kohl, U. (2022). What post-mortem privacy may teach us about privacy. *Computer Law & Security Review*, 47, Article 105737. <https://doi.org/10.1016/j.clsr.2022.105737>



Lopez, A. B. (2016). Posthumous privacy, decedent intent, and post-mortem access to digital assets. *George Mason Law Review*, 24(1), 183.
https://lawreview.gmu.edu/print_issues/24_gmlr_183/

Mali, P., & Prakash, A. (2019). Death in the era of perpetual digital afterlife: Digital assets, posthumous legacy, ownership and its legal implications. *National Law School Journal*, 15(1), Article 8.

Morse, T., & Birnhack, M. (2022). The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains. *New Media & Society*, 24(6), 1343–1362.
<https://doi.org/10.1177/1461444820974955>

Nwabueze, R. N., & White, M. (2026). Privacy law and the dead – a reappraisal (part II).

Journal of Media Law. Advance online publication.
<https://doi.org/10.1080/17577632.2026.2657763>

Öhman, C., & Floridi, L. (2017). The political economy of death in the age of information: A critical approach to the Digital Afterlife Industry. *Minds and Machines*, 27(4), 639–662.
<https://doi.org/10.1007/s11023-017-9445-2>

Öhman, C. J., & Watson, D. (2019). Are the dead taking over Facebook? A big data approach to the future of death online. *Big Data & Society*, 6(1), Article 2053951719842540.
<https://doi.org/10.1177/2053951719842540>

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1), Article ty001. <https://doi.org/10.1093/cybsec/>

