Preventing Unauthorized Use of Personal Data in Ghostbots Post-Mortem: An Access and Authorization Model for Digital Wills

Jasmin Bödecker, Jürgen Karla
Hochschule Niederrhein University of Applied Sciences, Faculty of Business Administration and Economics, NRW, Krefeld, Germany
jasmin.boedecker@stud.hn.de, juergen.karla@hs-niederrhein.de

The rise of AI-driven technologies, such as ghostbots, has introduced new challenges in digital legacy management, particularly regarding post-mortem data usage. A digital will can adress this challenge. Following the Design Science Research Method, this research proposes a structured access control model that enables Testators to define clear permissions for data access, inheritance, and the creation of ghostbots. The model integrates predefined roles and conditional access policies to ensure the Testators wisches regarding post-mortem data usage are met. The model is assessed by using logical proof and scenario-based evaluation. The findings highlight the necessity of robust access control mechanisms to prevent unauthorized use of personal data to enable ethical AI practices. By addressing these issues, this study contributes to the broader discourse on digital inheritance and ghostbots and provides an access control model framework for managing post-mortem digital identities through a digital will.

DOI
https://doi.org/10.18690/um.fov.4.2025.14

ISBN
978-961-286-998-4

Keywords:
ghostbots,
digital will,
post-mortem privacy,
personal data,
access control model

University of Maribor Press

1 Introduction

The accelerated development of artificial intelligence (AI) has enabled public access to popular systems such as ChatGPT. AI is becoming a part of multiple aspects of modern life, from autonomous driving to improving medical diagnoses (Kitzmann, 2022). The increasing use of technologies in the personal life, such as social media, results in vast amounts of personal, digital data. Such information encompasses personal data and digital identities that persist after a person's death, raising critical questions about how to manage, access, and ensure the security of these digital legacies. So far, there are no concrete regulations for what happens to a person's data when they pass away (Fuchs, 2021). Some companies such as Facebook or Google provide some kind of solution for this problem, like designating a person in charge of the account (Harbinja 2017). In most countries, after a person dies, the autonomy over their data dies with them (Harbinja 2022).

A recent development in AI systems are so-called "ghostbots". Ghostbots are generative AI systems that simulate the personality and behavior of deceased individuals (Figueroa-Torres 2024). There are different forms of ghostbots, ranging from chatbots to virtual avatars. They claim to allow the bereaved to continue interacting with their deceased loved ones. This development is discussed highly controversial and raises numerous ethical, legal, and psychological questions that need to be examined (Harbinja et al. 2023). For instance, the question arises whether an ethical use of ghostbots is even possible when the deceased have not given prior consent for their data to be used in these technologies. Harbinja et al. suggest a platform to manage consent for data usage in ghostbots (Harbinja et al., 2023).

2 Motivation

A digital will allows individuals to determine how their data is used after death, especially regarding ghostbots. It provides consent management, nominates responsible parties, and enforces user wishes across digital platforms. An access and authorization model is essential to govern interactions and prevent unauthorized data use (Harbinja, 2017).

3 Research question

This paper focuses on creating an access and authorization control model for a digital will platform as a concrete response to these aspects. It governs who has the authority to access, manage, or delete data after a user's death. This model must be comprehensive, secure, and adaptable to the various stakeholders involved.

Ghostbots operate by using personal data, including text messages, social media activity, voice recordings, and multimedia content (Lindemann 2022). While these systems hold the promise of comforting bereaved loved ones by allowing them to maintain a sense of connection with the deceased, they also pose significant risks (Jiménez-Alonso and Brescó de Luna 2023). Without adequate oversight and explicit consent from the deceased, the creation of ghostbots can lead to severe privacy violations, unauthorized exploitation of personal identity, and emotional harm to those grieving. Ghostbots can harm the bereaved by being used as a replacement for the deceased, leading to self-deception (Fabry and Alfano 2024) and even leading to addiction (Lindemann 2022). The more realistic the ghostbots, the higher the chance of addiction (Fabry and Alfano 2024) and the more difficult grieving becomes (Reese 2023). A possible risk is the deceased being portrayed inaccurately (Bao and Zeng 2024), creating further harm. Ghostbots allow bereaved to have a fictitious relationship with them (Fabry and Alfano 2024), creating new memories (Lindemann 2022) by enabling bi-directional communication (Jiménez-Alonso and Brescó de Luna 2023). Even though ghostbots allow open communication in private (Puzio 2023; Jiménez-Alonso and Brescó de Luna 2023), the important part of connection and support of others is neglected. Grieving with ghostbots can thus be isolating (Puzio 2023). Disrupting the grieving process can lead to prolonged grief disorder, causing those affected to be restricted in everyday life. This leads to a greater dependency on ghostbots, creating a vicious cycle (Lindemann 2022). To prevent these implications, a digital will can give the data owner the control over their data but also protect their beloved ones from these harms. The proposed access and authorization control model addresses these risks by giving individuals the ability to explicitly regulate the post-mortem use of their data. This allows for a tailored and ethical approach to digital legacy management. This balance between protection and ethical data use reflects the challenges posed by evolving AI technologies in the realm of digital inheritance.

4 Current State of Research

4.1 Digital Legacies and Data Ownership

Due to the increase of personal data, digital legacies have gained more importance (Cook et al. 2019; Cupar et al. 2023). A digital legacy can include digital assets such as social media profiles, photographs, text messages or audio files (Peoples and Hetherington 2015; Cook et al. 2019; Dissanayake and Cook 2019; Harbinja 2022). As mentioned before, there is considerable debate regarding the ownership of data after death. Often people misunderstand the ownership of their data once posted to a platform and assume digital assets are handled like physical assets (Cook et al. 2019). However, unlike physical property, digital assets are often governed by the terms of service of the platforms on which they reside, rather than by established inheritance laws (Fuchs, 2021). Additionally, these platforms each have individual policies, making it difficult to manage one's digital legacy (Cook et al. 2019). Harbinja arguments that digital assets should not necessarily be distinguished from physical assets. The lack of regulation leads to an unclear legal situation (Dissanayake and Cook 2019), allowing the bereaved to create ghostbots of loved ones, without prior consent. A universally accepted system is needed, not only for managing digital legacy (Dissanayake and Cook 2019), but for managing the growing popularity of ghostbots (Harbinja 2022).

4.2 Existing Solutions and Their Limitations

Within the European Union (EU) the General Data Protection Regulation (GDPR) sets regulations for data protection (European Parliament & Council of the European Union, 2016). The regulation specifies rights for data, including the right to deletion, restrictions on data processing, and access to personal data, which are particularly relevant to this research (European Parliament & Council of the European Union, 2016). In the context of ghostbots, the focus is on handling personal data of deceased individuals. Currently, many states lack specific laws regulating post-mortem data management, and it remains undetermined whether such data can be inherited or who holds rights over a deceased person's data.

4.3 Emerging Technologies: Ghostbots

A controversial development in digital legacy management is the emergence of ghostbots. To create ghostbots, personal data is used to recreate the voice, look, personality, and behavior of deceased individuals (Puzio 2023). While this technology may offer solace to some grieving individuals, it raises ethical questions (Puzio 2023). If ghostbots are created without the explicit consent of the deceased, this could be considered a serious violation of privacy. Moreover, there is a risk of psychological harm to the bereaved, who might struggle to cope with the simulation's realism (Harbinja et al., 2023).

Compared to other forms of remembrance such as videos or photos, ghostbots allow two-way communication. This allows new memories being formed, which otherwise would not have been possible (Puzio 2023).

4.4 Access and Authorization Control Models

The purpose of access control is to restrict data access to authorized entities only, ensuring the protection of information and preventing any potential misuse (Tsolkas and Schmidt 2017). In the context of an access control model, it is important to differentiate the terms authentication, authorization and access control (Mahalle et al. 2022). Authentication describes the identification of a user, while authorization sets rules which specify which actions a user is allowed to perform (Chen et al. 2009; Boonkrong 2020). Based on the authorization policies, access control then allows access to data or systems (Tsolkas and Schmidt 2017).

Building an effective access control model involves structuring a framework that manages how and when subjects can interact with objects (Tsolkas and Schmidt 2017). Subjects can be users or other systems and object different types of data. Central to this model are roles and permission levels, which define what actions each user can perform based on their responsibilities or identity. For example, in a role-based access control (RBAC) system permissions are assigned to roles rather than to individual users, streamlining the management of access rights (Ferraiolo and Kuhn 1997; Chen et al. 2009; Gupta et al. 2022). A more advanced, dynamic model might incorporate dynamic attributes to adapt permissions in real-time (Atlam et al. 2020; Pal 2021). These attributes can include time, location or events. The success

of an access control model relies on its ability to balance security with usability. Permissions should be clearly defined to prevent unauthorized actions, while still allowing legitimate users efficient access. The core elements must be precisely managed through well-established policies, ensuring that only authorized entities can perform actions.

5 Method

The research methodology chosen for this study is the Design Science Research Method (DSRM) (Hevner et al. 2004; Peffers et al. 2007). This structured approach allows the development of practical and innovative solutions to complex problems.

The first step identifies the problem, highlighting the challenges posed by AI technologies like ghostbots in digital legacy management. A structured literature review established the problem's relevance and the need for a solution. The second step defined objectives, aiming to develop a secure, flexible, and ethical access control model that ensures compliance with the deceased's wishes. The third step involves designing and developing the model, including role definitions and access control policies with a focus on ethical AI use. This is followed by demonstrating the model's functionality, showcasing predefined roles, conditional access enforcement, and consent management. The fifth step evaluates the model's effectiveness through theoretical consistency checks and thought experiments to ensure scalability and precision.

6 Artefact

Ghostbots are being created without the explicit consent of the deceased, raising significant ethical concerns. Additionally, there is a lack of clear directives for handling digital assets post-mortem, including consent to ghostbots. Since digital assets are typically not included in traditional wills, there is no consistent regulation governing the management of personal data after death. Existing platform policies vary widely, are often ambiguous, and lack standardization. A digital will presents a potential solution for individuals to manage their digital data posthumously and prevent ghostbots from being created unethically.

- The objective of this paper is to design an access and authorization control model for a digital will. The model's design requirements (DR) are derived from platform functions and relevant literature as follows:DR1: The model must precisely control which subjects can access specific kinds of data.
- DR2: The model must allow a structured and scalable access management.
- DR3: The access control model must include mechanisms for conditional access.
- DR4: The user should be able to control the consent management.

6.1 Access and Authorization Model

Access control models are frameworks designed to regulate who can access specific resources, what actions they can perform, and under what conditions (Salim et al. 2010; Tsolkas and Schmidt 2017; Boonkrong 2020). These models form the foundation of any secure system, providing mechanisms to enforce permissions and ensure that data, especially personally identifiable information remains protected from unauthorized use or manipulation (Larson 2022). For the digital will platform, a hybrid approach between RBAC and dynamic features is the most suitable. RBAC ensures a clear and scalable role definition for Testators, heirs, and platform administrators, while dynamic elements allow the inclusion of conditional access policies. This combination aligns the platform's needs for clarity and adaptability, ensuring sensitive data is managed securely while accommodating the individual needs of post-mortem data management.

Firstly, the basic parts of an access control model need to be defined. These consist of subjects, objects and actions. Based on the requirements described previously, there are two types of subjects. Subjects refer to both the human users, as well as non-human users. These can be other systems or third-party platforms, that interact with the platform. The primary subjects will have higher privileges and access rights. The data owner controls the rules for the other users. Even when they are no longer actively using the system, their consent and wishes dictate access policies. Followed by the data owner, the primary executor would be the next user in hierarchy. A primary executor is a trusted person, in charge of managing the deceased data according to their digital will. A legal representative has authority over data when legal obligations or disputes need to be handled. A legal representative can also be a

primary executor. These rolls are defined by the data owner. Secondary subjects have limited or specific privileges in comparison to primary subjects. The secondary subjects can be divided into three categories, family members or next of kin, friends and third-party platforms. The third-party platforms can be differentiated into platforms with and without the use of AI. More specifically, platforms which main purpose is to use the deceased data to create ghostbots. Family members or friends have limited access rights based on the deceased preferences while access for third-party platforms is restricted to automated, API-based communication.

Objects are the data or resources that need to be protected and controlled within the platform. It is important to understand the types of data and their sources, to allow appropriate mapping between the objects and subjects. Furthermore, this helps define actions permissible for each relationship. There are different types of data, accumulating from different sources, creating digital identities. Data is not limited to text, audio and visual, but can include metadata, data from digital entertainment, search histories, financial data and any other data that is created using platforms. The different types of objects, or data, can come from different sources. The data owner can upload content directly to the platform. Otherwise, data can be imported through cloud storage, social media platforms or other types of accounts.

It is important to differentiate data by type and source. Being able to give precise permissions for different types of data, allows granular control. It adds scalability, as new data types or sources can be incorporated without restructuring the entire system. This categorization directly influences the design of the access control model. Categorizing data by type and source helps tailor an access control model to ensure that specific roles access only the data relevant to them. Incorporating dynamic features and defining subject-object relationships further refine the model, enabling conditional and precise management of actions allowed for each user role. Actions are operations that subjects can perform on objects. These actions are detect, search/find, compare, show, read, add, change, delete and execute (Tsolkas and Schmidt 2017). These actions can be assigned to the individual roles and be restricted by conditional access. Privileges are the specific permissions granted to subjects to perform actions on objects. These are linked to the subjects' roles.

6.2 The Access Control Model

Predefined roles serve as the foundation of this system, each with default settings aligned with the purpose of the platform and the ethical considerations of post-mortem data management. These roles are categorized into primary roles, which hold the highest levels of responsibility and access, and secondary roles, which are more limited in their permissions. Additionally, third-party platforms are integrated through controlled API connections, ensuring that their access is tightly regulated and specific to predefined tasks.

Primary and Secondary Roles

Primary roles include the Primary Executor and the Legal Representative, both of whom are entrusted with high levels of access but are distinguished by their specific responsibilities.

Secondary roles include the Heir, Next of Kin as well as Additional Individuals. They are provided with restricted access to specific data categories and actions. Table 1 displays the different roles and default actions. The primary and secondary roles do not include system roles, since system roles are not controlled by the Testator. The platform administrator is a system role. This role is responsible for maintaining the platforms functionality and does not have access to the user's personal data. Access is highly restricted and focuses on maintenance, policies and security rather than managing the digital will of people.

The dynamic features enhancing the RBAC framework, allow users to adjust the default permissions to suit their unique circumstances. For instance, the Primary Executor or Heirs may receive conditional access that activates upon the confirmation of death or at specific time intervals. Granular control enables the data owner to define permissions for each role at a detailed level, such as allowing an Heir to view financial records while restricting access to personal emails. This flexibility ensures that the platform can adapt to individual preferences while maintaining the integrity and security of sensitive data.

Table 1: Primary and Secondary Roles

Role	Who	What	When
Testator	User creating their will	Create, Edit and delete digital will, define access control for individuals, view access protocols	Always
Primary Executor	Individual chosen by Testator	Full Access, execute will	After legal confirmation of Testators death, active until completion of will
Legal Representative	Lawyer, notary or legally appointed individual	Validate and confirm will, conditional access only for legal processes	Access triggered by predefined legal needs, expires once needs are completed
Heir	Individuals	Medium Access, view data and perform actions based on the will	Access begins with confirmation of Testators death, expires once inheritance-related tasks are completed
Next of Kin	Family Members	Limited Access, view only	Access triggered by confirmation of Testators death, Access remains indefinitely
Additional Individuals	Friends, Colleagues, Acquaintances	Limited Access, Highly specific, view-only access	Access triggered by confirmation of Testators death, Access remains indefinitely

Third-Party Platforms

Third-party platforms are incorporated into the access control model through APIs. These entities do not interact directly with the platform or its users but receive automated instructions to perform specific tasks. Their access is conditional and highly restricted, ensuring they can only complete the tasks defined by the user's will and cannot access or manipulate unrelated data. The default settings for third-party platforms are show in Table 2.

A critical function of the digital will platform is to provide users with comprehensive control over whether or not a ghostbot be created. Not only should the user be able to make the decision if, but with what data a ghostbot can be created. The access granted in the digital will should reflect the Testators consent and permissions. This control extends beyond approval for creation, but dictate what data can be used,

who can interact with the ghostbot, how long it should exist, and in what form it should be presented.

Table 2: Third-Party Platforms

Type of Third-Party Platform	Who	What	When
Social Media	Social Media Platforms	Delete/deactivate account	Triggered by confirmation of Testator's death
Email Accounts	Email Service Providers	Create and save backup, delete account	Triggered by confirmation of Testator's death
Cloud Storage	Cloud Service Providers	Create Backup, Transfer Ownership	Triggered by confirmation of Testator's death
Financial Accounts	Banking platforms	Transfer ownership	Triggered by confirmation of Testator's death
Ghostbots	Ghostbot Platforms	No Access	Triggered by confirmation of Testator's death

The platform places the decision to permit or deny the creation of a ghostbot entirely in the hands of the data owner. During their lifetime, users can specify whether they wish to allow the generation of a ghostbot after their passing. This decision is reflected in the access, by allowing no access. For those deciding for a ghostbot, the platform allows detailed access policies. The user can define which types of their data are to be utilized in generating the ghostbot's personality, communication style, and responses. Additionally, the platform extends to manage who can interact with the ghostbot. Users can assign specific roles to their chosen heirs, family members, or other individuals, determining who has the privilege to access the ghostbot. For instance, the data owner might decide that only close family members can engage with the ghostbot, while more distant acquaintances have no access. These permissions are managed with the same rules as the broader access control features. This ensures that interactions with the ghostbot align with the user's intent. This can prevent misuse of the ghostbot. Moreover, the platform allows users to establish time-based constraints on the ghostbot's existence. As mentioned previously, data is usually bound to a certain context. By adding time-based constraints to the ghostbot, it can be avoided to create a ghostbot, that is contained in its social context and timeline. This capability helps to decrease ethical concerns regarding the indefinite

representation of individuals who have passed away, which could lead to unintended consequences over time. Equally important is the ability for users to define the scope and format of the ghostbot. For example, some users might want the ghostbot to convey only curated messages for memorial purposes, while others may allow more dynamic and personalized interactions based on their historical data.

All these decisions are enforced by the access control model, which ensures that only authorized actions are carried out. If the data owner wishes to revoke permissions for the creation or use of the ghostbot, the platform must immediately halt any associated processes and restrict access to the relevant data. Likewise, interactions between the ghostbot and third-party platforms, such as social media networks or external applications, are mediated through secure API integrations, adhering strictly to the data owner's established preferences. By providing users with detailed and transparent tools to manage the creation and use of ghostbots, the digital will platform upholds the principles of consent, autonomy, and ethical responsibility. It ensures that these AI representations serve as an extension of the data owner's wishes, rather than a violation of their legacy, fostering trust and accountability in this sensitive area.

7 Logical proof

The basic function of the model is allowing a user precise control over the access to their data (DR1). The model is based on roles with access permissions for specific actions and specific objects. The objects represent the different types of data, subjects refer to the people designated to have access to the objects and actions. Enforcing the permissions through roles ensures that only authorized people can perform actions. The differentiated kinds of objects allow the user to specify actions with a high level of granularity. Additionally, conditional access controls that access is only activated once the user passes away. For example, a friend of the user could receive access to selected photographs, while the heir receives access to all images.

Structured and scalable access management (DR2) is another essential design requirement. The role-based architecture enables a simple structure, reducing ambiguity in access control. This inherently provides structure because roles encapsulate predefined permissions for specific actions on specific data. Additionally, it supports scalability, since new roles and permissions can be added to

the system without redesigning the entire framework. For this requirement, the dynamic features allow further structurization of access model, such as time limits for data access. For example, if a user wants to add more people to the will, they would be added to the role "additional individual" with limited access as a default. The user can then add individual permissions, with time constraints such as "view images for 4 weeks".

As mentioned before the dynamic features enable the user to add conditions to permissions (DR3). The roles act as baseline for permissions while conditional access mechanisms refine them. Conditional access can include time-related conditions or event-driven conditions. One crucial event-driven condition being the legal confirmation of the user's death. This ensures that the digital will is only activated when necessary, preventing misuse of data.

The fourth design requirement focuses on consent management, especially in context to ghostbots (DR4). Consent is managed through the access that third-party platforms creating ghostbots receive. The first step is deciding for or against ghostbots. If the user decides against it, access is denied. If creation of ghostbots is allowed, access can be granted granularly for the different types of data or third-party platforms. This way, the user is in control of how he is portrayed. Additionally, the dynamic features can limit the time, the ghostbots exists or who can have access. This could lower the risks for the bereaved that can occur when the creation and access to ghostbots is not controlled.

8 Discussion and limitations

The proposed model gives insight to a small part of the digital will. Future research should explore the security measures that can be implemented, to ensure the safety of personal data against potential threats. Improving user verification through two-factor authentication could significantly improve user verification. Temporary access keys that expire after usage could further strengthen security. To provide transparency and accountability, all user actions should be strictly logged. Access to critical system components by the platform administrator could further be restricted through VPN. The frontend should be intuitive and accessible, both for the Testator and the people who have been given access to the will. It should be evaluated, to

what extend guidance and tips are necessary, both for the Testator to make informed decisions, but also to enable users' easy guidance during grief.

The proposed access control model fulfills the requirements, describes, and demonstrates potential for a digital will platform. It addresses precise control over data, scalability and conditional access, especially in context of ghostbots. However, there are several limitations that must be acknowledged. Differences in legal frameworks, cultural norms and technological adoptions across countries lead to significant issues. This lack of consistency in international regulation complicates the implementation of a universal digital will. Digital assets and posthumous data management need to be regulated on a governmental level, before a digital will can be implemented. Without mandates or regulations requiring platforms to integrate the digital will, gaps in coverage are to be expected. To ensure that a digital will is executed, coordinated legislative action is required. This is currently lacking.

One of the biggest limitations concerns ghostbots specifically. Individuals can still create ghostbots using private data they have, without oversight. Even though the user decision against ghostbots could be grounds for legal action against otherwise created ghostbots, it is difficult to find those ghostbots. Through this loophole, the control mechanisms of the platform can be undermined. A mandatory check between ghostbot platforms and the digital will, could close this gap, however the risk remains. This could lead to ethical issues or even misrepresentation of the deceased. Addressing these issues will require a combination of regulatory interventions, increased public awareness, and platform accountability to ensure the digital will system functions as intended and respects the complexities of diverse user needs and contexts.

The model proposed offers great detail in customizing access. While the model does support scalability, the growing number of users and data may require additional infrastructure. Additionally, conditional access strengthens security, however it also introduces complexity. This could lead to misconfigurations if not implemented carefully. Third-party platforms are connected using APIs. Although it enhances functionality, it can expose vulnerabilities. Especially due to the nature of the data, compromised security is a great risk.

9 Conclusion

There is a growing need for ethical posthumous data management. Developing an access model, gives insight to a digital will platform addressing this issue. The proposed model incorporates roles, different types of media and dynamic feature for conditional mechanisms. However, significant challenges remain. The rapid developments and lack of unified legal regulations create challenges that a digital will cannot overcome. These issues highlight the need for regulatory mandates that compel digital platforms to integrate with digital will systems to ensure comprehensive coverage. There is need for ongoing education about personal data, one's digital footprint and new AI-technologies such as ghostbots. Ghostbots especially introduce ethical, legal and privacy concerns. Possible unauthorized ghostbots violate the deceased and pose risks for the bereaved.

While the proposed access control model outlines a possible foundation for managing digital legacies, the success depends on collaboration with and between governments, providers of platforms and ghostbots. Addressing the risks associated with emerging technologies like ghostbots and ensuring ethical oversight are critical. With continued refinement, adaptation to legal and technological changes, and a focus on accessibility, the platform has the potential to set a standard for ethical and secure posthumous data management in the digital age.

References

Atlam HF, Azad MA, Alassafi MO, et al (2020) Risk-based access control model: A systematic literature review. Future Internet 12:. https://doi.org/10.3390/fi12060103

Bao A, Zeng Y (2024) Embracing grief in the age of deathbots: a temporary tool, not a permanent solution. Ethics Inf Technol 26:. https://doi.org/10.1007/s10676-024-09744-y

Boonkrong S (2020) Authentication and access control: Practical cryptography methods and tools. Apress Media LLC

Chen TY, Chen YM, Wang C Bin, Chu HC (2009) Flexible authorisation in dynamic e-business environments using an organisation structure-based access control model. Int J Comput Integr Manuf 22:225–244. https://doi.org/10.1080/09511920802209041

Cook DM, Dissanayake DN, Kaur K (2019) The Usability factors of lost Digital Legacy data from regulatory misconduct: older values and the issue of ownership. International Conference on Information and Communication Technology (ICoICT) 105

Cupar D, Ivanović MD, Grgeč A (2023) Personal digital legacy: Findings from an exploratory study among citizens of Croatia. Education for Information 39:517–540. https://doi.org/10.3233/EFI-230057

Dissanayake DN, Cook DM (2019) Social computing and older adults: Challenges with data loss and digital legacies. In: Proceedings - 2019 International Conference on Cyberworlds, CW 2019. Institute of Electrical and Electronics Engineers Inc., pp 171–174

Fabry RE, Alfano M (2024) The Affective Scaffolding of Grief in the Digital Age: The Case of Deathbots. Topoi. https://doi.org/10.1007/s11245-023-09995-2

Ferraiolo D, Kuhn DR (1997) Role-Based Access Control

Figueroa-Torres M (2024) Affection as a service: Ghostbots and the changing nature of mourning. Computer Law & Security Review 52:105943. https://doi.org/10.1016/J.CLSR.2024.105943

Gupta M, Bhatt S, Alshehri AH, Sandhu R (2022) Access Control Models and Architectures For IoT and Cyber Physical Systems. Springer International Publishing

Harbinja E (2017) Post-mortem privacy 2.0: theory, law, and technology. International Review of Law, Computers and Technology 31:26–42. https://doi.org/10.1080/13600869.2017.1275116

Harbinja E, Edwards L, McVey M (2023) Governing ghostbots. Computer Law and Security Review 48:. https://doi.org/10.1016/j.clsr.2023.105791

Harbinja Edina (2022) Digital Death, Digital Assets and Post-Mortem Privacy. Edinburgh University Press

Hevner, A.R., March, S.T., Park, J., Ram, S. (2004) Design Science in Information Systems Research. MISQ. 28:75–105. https://doi.org/https://doi.org/10.2307/25148625

Jiménez-Alonso B, Brescó de Luna I (2023) Griefbots. A New Way of Communicating With The Dead? Integr Psychol Behav Sci 57:466–481. https://doi.org/10.1007/s12124-022-09679-3

Larson JM (2022) Snowflake Access Control: Mastering the Features for Data Privacy and Regulatory Compliance. Springer

Lindemann NF (2022) The Ethics of 'Deathbots.' Sci Eng Ethics 28. https://doi.org/10.1007/s11948-022-00417-x

Mahalle PN, Bhong SS, Shinde GR (2022) Authorization and Access Control. In: Authorization and Access Control. CRC Press, pp 19–31

Pal S (2021) Internet of Things and Access Control: Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems. Springer Nature Switzerland AG, Cham

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. Journal of Management Information Systems 24:45–77. https://doi.org/10.2753/MIS0742-1222240302

Peoples C, Hetherington M (2015) The Cloud Afterlife: Managing your Digital Legacy. IEEE International Symposium on Technology and Society (ISTAS) 1–7

Puzio A (2023) When the Digital Continues After Death. Ethical Perspectives on Death Tech and the Digital Afterlife. Communicatio Socialis 56:427–436. https://doi.org/10.5771/0010-3497-2023-3-427

Reese A (2023) The rise of grief tech. New Sci (1956) 41–43

Salim F, Reid J, Dawson E (2010) Towards Authorisation Models for Secure Information Sharing: A Survey and Research Agenda. In Press

Tsolkas A, Schmidt K (2017) Rollen und Berechtigungskonzepte Identity- und Access-Management im Unternehmen