

Post-mortem information management: exploring contextual factors in appropriate personal data access after death

Jack Holt, Jan David Smeddinck, James Nicholson, Vasilis Vlachokyriakos & Abigail C. Durrant

To cite this article: Jack Holt, Jan David Smeddinck, James Nicholson, Vasilis Vlachokyriakos & Abigail C. Durrant (21 Jan 2024): Post-mortem information management: exploring contextual factors in appropriate personal data access after death, Human-Computer Interaction, DOI: [10.1080/07370024.2023.2300792](https://doi.org/10.1080/07370024.2023.2300792)

To link to this article: <https://doi.org/10.1080/07370024.2023.2300792>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



View supplementary material [↗](#)



Published online: 21 Jan 2024.



Submit your article to this journal [↗](#)



Article views: 273



View related articles [↗](#)



View Crossmark data [↗](#)

Post-mortem information management: exploring contextual factors in appropriate personal data access after death

Jack Holt^a, Jan David Smeddinck^{a*}, James Nicholson^b, Vasilis Vlachokyriakos^a, and Abigail C. Durrant^a

^aOpen Lab, Newcastle University, Newcastle upon Tyne, UK; ^bComputer and Information Sciences, Northumbria University, Newcastle upon Tyne, UK

ABSTRACT

With the increasing size and complexity of personal information and data landscapes, there is a need for guidance and support in the appropriate management of a deceased person's postmortem privacy and digital legacy. However, most people engage poorly with existing mechanisms for specifying and planning for access and suitable usage of their own data. We report on two studies exploring the ways in which contextual factors such as the accessor and the data type may affect the appropriateness of personal data flows differently during life and after death. Our findings indicate that suitable data access after death is highly individual and contextual, with differences in appropriateness between during-life and after-death data flows significantly affected by the accessor and the data type in question. We identify that ambiguous accessor motivation, failure to communicate intent, changing temporal context and latent data values further complicate the act of digital legacy planning. Our findings also provide further evidence for the existence of a postmortem privacy paradox in which reported user behaviors do not reflect intent. With this in mind, we offer design recommendations for the integration of digital legacy planning functionality within Personal Information Management (PIM) and Group Information Management (GIM) systems.

ARTICLE HISTORY

Received 28 October 2022
Revised 16 November 2023
Accepted 15 December 2023

KEYWORDS


Digital legacy; post-mortem privacy; personal information management; group information management; privacy

1. Introduction

In recent years, the quantity of digital personal information that is generated and stored has become large, dispersed, and arguably difficult to manage. Through their engagement with different tools and services, technology users create and must navigate their own complex personal data landscape (Bowyer et al., 2022). The last decade has seen several high-profile and large-scale data misuses, including the widespread multi-nation government intrusions on personal data revealed by the 2013 Snowden leaks (Greenwald et al., 2013) and the political interference enabled by improperly accessed Facebook user data in the Facebook-Cambridge Analytica scandal several years later (Cadwalladr & Graham-Harrison, 2018). This has led to increased public and political focus on data protection and privacy. The EU's General Data Protection Regulation (GDPR) came into force in 2018, aiming to support individuals' rights with respect to their personal data and protect them from data misuse (European Union, 2016). However, such rights and regulations usually relate to living individuals, not the dead. The access that those who are living have, or should have, to a person's personal data

CONTACT Jack Holt  j.holt3@newcastle.ac.uk  Open Lab, Newcastle University, Newcastle upon Tyne, UK

*Current affiliation for Jan David Smeddinck: Ludwig Boltzmann Institute for Digital Health and Prevention.

 Supplemental data for this article can be accessed online at <https://doi.org/10.1080/07370024.2023.2300792>

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

after death (referred to henceforth as *post-mortem data*) remains a gray area both morally and legally (Michels et al., 2019; Stokes, 2015). Loved ones tend not to have official permission to access personal data of a deceased person, but may (or may not) have access through known/shared passwords. There remains a question of what kinds of data access would the deceased have permitted if they were able to assess these postmortem circumstances of access for themselves. Prior work in Human-Computer Interaction (HCI) and related fields has indicated that views on the treatment of postmortem data vary between individuals, but this has largely been focussed on preferred digital legacy outcomes (Grimm & Chiasson, 2014; Morse & Birnhack, 2020; Nakagawa & Orita, 2022). Absent from these preferences is consideration of how individuals would prefer or expect potential accessors to behave in the absence of defined plans, or how nuanced contextual factors might influence the appropriateness of postmortem data access under such circumstances. In particular, we identify a need to understand views on whether the death of an individual renders intrusion on their data privacy by others more appropriate, and on what basis.

Within Personal Information Management (PIM) systems, we see a need for designs that better support long-term and postmortem futures of data. These should support users to identify parts of their own personal data landscape which they would prefer to become accessible and understandable to others in the future, as well as those parts for which they would prefer reduced access or destruction. PIM primarily focuses on how information can be stored, organized, and retrieved by the user themselves, often using a directory structure known only to them (Jones et al., 2001; Lush, 2014). Group Information Management (GIM) focuses on shared data repositories in which information is accessed and edited by multiple parties, often at a cost to efficiency and ease of access (Bergman et al., 2014; Lutters et al., 2007; Markus, 2001). We identify a digital legacy context in which information stored by one user goes on to potentially be perused or retrieved by another user – a space somewhere between PIM and GIM. However, there also exists a substantial part of a person's information landscape that is generated through observations of their technology interactions, derived or estimated about them through data analysis, or collated from other sources (Bowyer et al., 2022). Whilst these data may exist outside of the awareness of most users, they nevertheless have the potential to impact digital legacy and postmortem personal privacy.

This paper reports on mixed-methods research exploring the social acceptability of different forms of postmortem access and the expectations that people have about how their own personal data is accessed and used after their deaths. Firstly, using a questionnaire ($N = 108$), we investigated the extent to which people perceive the appropriateness of unauthorized data access to their own personal data to change in the event that the access takes place when they are no longer living. In particular, we sought to understand how contextual factors such as “what” the type of data is and “who” is accessing might affect such judgments, basing our approach on the Contextual Integrity model of information privacy (Nissenbaum, 2004, 2009). Secondly, we conducted and analyzed semi-structured interviews ($N = 12$) to examine individual rationales and motivations that underpin such judgments of appropriateness, seeking to understand personal evaluations of future data values and privacy and how they shape expectations around postmortem privacy boundaries. Additionally, we collected overall privacy and postmortem privacy valuations and protection behaviors in order to identify any disconnect between intent and behavior, which has previously been identified as a postmortem extension to the established *privacy paradox* phenomenon (Norberg et al., 2007), in which people are seen to display concern about their privacy but fail to act appropriately to protect it (Holt et al., 2021; Morse & Birnhack, 2020).

Through descriptive and inferential analysis of the questionnaire data and a thematic analysis of the transcribed interviews, our findings paint postmortem data access values as highly individual and contextual, with death representing a change in perceived appropriateness for some, but not all, participants. Appropriateness of unauthorized postmortem data access and willingness to give permission for that access were seen to differ depending on the type of data and who the accessor would be, indicating a need for integration of context and data granularity within plans for postmortem data access. Our results also support the

presence of a postmortem privacy paradox, with participants reporting that they consider postmortem privacy to be important yet expend little effort to protect it. In this paper, we will report on our findings to ground an argument that PIM does not yet adequately support the consideration of postmortem information, suggesting implications for the design of tools and processes that support the formulation of legacy plans of sufficient granularity and individuality.

2. Background

2.1. Data values

With the growing prevalence of digital devices and services, it is becoming common for people to generate, intentionally or otherwise, large sets of data relating to their daily lives. The capture and usage of this data is a powerful tool for change and a driving factor in the success of today's largest online businesses, and as a result of increasing public awareness of past and potential misuses of user data, recent years have seen a push for clearer data collection and usage policies and user settings. Human-Data Interaction (HDI) is an interdisciplinary field of study that places humans at the center of their data, formed around themes of *legibility* (relating to transparency of collection and usage policies), *agency* (relating to the capacity of users to take action within data systems) and *negotiability* (relating to users' ability to react to dynamic elements of data access and changing social norms) (Mortier et al., 2014). Similarly, Acquisti et al. (2015) use three themes to connect privacy research: *uncertainty*, in which technology users are unsure to what degree they should be concerned about privacy (often due to asymmetric information or understanding about how personal data is collected and used); *context-dependence*, in which views on privacy fluctuate with context and according to environmental and social cues; and *malleability*, in which behavioral and psychological processes may be used to impact privacy behaviors of users. The GDPR has provided many users with the legal right to understand what is being collected about them and how it is used, access the personal data that organizations collect and store about them, request the erasure of their personal data, and to object to particular personal data processing that is not related to the service in question (European Union, 2016). Elsewhere, similar regulations have emerged, such as the 2018 California Consumer Privacy Act (CCPA) (Kessler, 2019). Whilst compliance and effectiveness of these processes has been limited, many large companies have since introduced tools that allow users to easily download copies of their personal data (Bowyer et al., 2022).

Alongside the big data interests of major corporations and governments, and the associated power shifts that have become associated with them (Zuboff, 2015), there is also value and meaning to be found within individual data trails. Data, digital possessions and shared online spaces can play a role in the way that people construct and co-construct their sense of self (personal identity) (Belk, 2013), and social media can be used as a means of constructing alternate digital identities to be presented to others (Hogan, 2010). *Personal informatics* is a field of study relating to self-tracking through data, which is an activity that people may carry out in order to inform behavior change or simply to know themselves better (Li et al., 2010). Epstein's model of *Lived Informatics* describes associated decisions and behaviors associated with personal informatics, including tool selection, reflection and lapsing of tracking behaviors (Epstein et al., 2015). The *Quantified Self* movement represents the cultural phenomenon of using personal informatics to derive self-knowledge (Lupton, 2016), which can ultimately result in a personal historical record from which a person – or their loved ones – might derive value and meaning (Elsden & Kirk, 2014; Elsden et al., 2016). However, some argue for such technology to support narratives and meaning-making above simply representing the “facts” of a person's life (Crete-Nishihata et al., 2012). With respect to health data, the 2022 European Health Data Space proposal aims to create an ecosystem in which citizens are supported to control their own data on an individual level whilst also contributing to the use of that data on a wider scale within research and policy making (European Commission, 2022). An emerging area of development

with respect to distributed online personal data and informatics is the use of personal data stores (PDS) as a means of re-imagining data flows between users and services and supporting negotiability of data access (Fallatah et al., 2023).

We also consider, herein, the potential value of such individual data after death, whether collected by an individual or a third-party, alongside potentially conflicting privacy expectations and norms.

2.2. *Post-mortem privacy*

In this paper we will use the term *post-mortem privacy*, referring broadly to the concept of privacy after death. As such, we align with Edwards and Harbinja, who speak of “the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after death” (Edwards & Harbinja, 2013). Our treatment of privacy, more generally, builds on the concept of Contextual Integrity (Nissenbaum, 2004); we consider privacy not as a static attribute that can be applied to a particular dataset, but rather in terms of the appropriateness of *data flows*. For Nissenbaum, privacy is rooted in the flow of data from one place to another, and a data flow can be described in terms of contextual factors such as who the subject, sender and recipient are, what the data are, and under what transmission principle (such as consent) information is sent. In a series of quantitative works on the subject, Martin and Nissenbaum used *factorial vignettes* (scenarios that vary according to a factorial experimental design) to explore how variations in these contextual factors profoundly impact privacy evaluations of ostensibly “sensitive” information (Martin & Nissenbaum, 2016), discredit the notion of a dichotomy of public versus private data (Martin & Nissenbaum, 2017), and reveal location data to be a category of personal data for which privacy depends a great deal on contexts of access and usage (Martin & Nissenbaum, 2019). Across those findings, the authors describe commercial uses and mass collection and sale by data brokers to be among the most contentious, even for data that may already be publicly available. In this work we consider the *vital status* of a person (which is to say if they are alive or dead) as a potential part of the context of a data flow. For example, an individual may consider it appropriate for financial data to be provided to their executor once they are dead, but not before. Further, we identify that vital status may be a relevant factor not only in the appropriate access of data, but also its usage. For example, Bassett (2022) proposes that with advancements in technology, there may come a need for a Digital Do Not Re-Animate (DDNR) order, so that people may prevent data relating to them being used in order to falsely represent them posthumously. Similarly, there are calls for an enforceable clause in wills in support of the dignity and privacy interests of an individual to prevent or otherwise control acts of digital reincarnation (Harbinja et al., 2023), or to expand legislation to safeguard against unauthorized digital cloning (Roberts, 2023). Just as the notion of individual privacy may spill over into wider societal issues such as surveillance capitalism (Zuboff, 2015), we view postmortem privacy as having the potential to safeguard against other postmortem consequences that may oppose a person’s interests.

There has been limited research investigating user perspectives on the future of their data and data privacy. Grimm and Chiasson (2014) examined how 400 participants of various nationalities felt their digital footprints should be handled after death. They found participants to exhibit a wide range of opinions on the value of planning for death and for planning for digital legacy specifically. Of the options given to participants, the three most popular, in order, were deletion, passing to the next of kin and deciding individually (for each asset/account), all of which were considered preferable to leaving things as they were, going by the terms of service, or making data public. When asked about specific accounts, those related to banking, cloud storage, blogging and photography were most commonly preferred to be transmitted to the next of kin, whilst those relating to social media, e-mail, chat, entertainment, contributions to collaborative websites, shopping, dating, gambling, and government were most commonly preferred to be deleted. However, in most cases, each specific form of account garnered a range of preferences. Qualitative work by Pfister (2017) also indicates a tendency toward deletion for the majority of a person’s data and accounts. In another survey,

participants were seen to be split between three broad options: “deny access to all contents”, “allow access to some of the content” and “allow access to all contents” (Morse & Birnhack, 2020). Across three main types of content (e-mail, SNS and cloud), their participants differed only slightly, with, in each case, about one fifth preferring access to “some” content, about one third preferring to deny all access, and about half preferring to allow all access. Most preferred such access to be granted to their spouses, if anyone, followed by parents and children as applicable. The reasons for such access, as reported using open-ended questions, were seemingly focused on providing important information enabling others to make arrangements, supporting memories and commemoration, and leaving things of a sentimental nature. When asked why they would deny such access, participants’ main reasons related to privacy, with some simply considering such things to be irrelevant after death. A more recent survey by Nakagawa and Orita (2022) placed a particular emphasis on potential commercial usage. They saw a tendency toward preferences for automatic deletion of internet services usage data for both real-name and anonymous accounts, and when asked if they would nominate a particular person to be able to manage or read their personal data from these services, more than 50% either did not want to nominate somebody or did not have somebody suitable to nominate, with those who did nominate an individual typically choosing a spouse, child or sibling. Presenting various forms of postmortem data usage, they found that most were deemed unacceptable, even if they or their heirs were to be financially compensated for the usage. Yet, even when individuals appear to value continued privacy after death, it has been observed that actions tend not to reflect this – a postmortem extension of the privacy paradox phenomenon (Holt et al., 2021; Morse & Birnhack, 2020). Morse and Birnhack (2020) describe a posthumous privacy paradox in terms of three user groups: those for whom the privacy paradox persists posthumously, those who resolve the paradox by making plans, and those for whom there is an inverted paradox, in which users wish to share their data posthumously but fail to act in support of that preference.

2.3. Digital legacy

In recent decades, the topic of what we leave behind of our digital lives has been studied across multiple disciplines. In Law, scholars have sought to unpick the evolving nature of digital assets as property, and legislate when and how digital entities may be inherited and the extent to which personal privacy and data protection regulations ought to apply (Birnhack & Morse, 2022; Harbinja, 2022). In some jurisdictions, access to digital assets for fiduciaries where specified in one’s will is legislated (RUFADAA in most of the United States (Fiduciary Access to Digital Assets Act, Revised, 2015), UADFA in Canada (Uniform Law Conference of Canada ULCC, 2016), and France’s Law for a Digital Republic (Gouvernement de la République française, 2016), however this is typically restricted to those who have taken legacy planning actions and does not necessarily simplify the matter from a technological, privacy or organizational standpoint. Psychologists and sociologists have observed changing practices of mourning and memorialization with the proliferation of social media (Brubaker et al., 2013; Kasket, 2012, 2019; Walter, 2015). Within fields also engaging Engineering and Computer Science, such as HCI and Cybersecurity, a wide range of research has explored issues involving how users may design, curate or otherwise plan their *digital legacies*, and how their legacy may go on to affect others (Chen et al., 2021; Gulotta et al., 2013, 2017; Maciel, 2013; Maciel & Pereira, 2015; Odom et al., 2012). Digital legacy research also includes explorations of the postmortem transfer of access to (or destruction of) digital assets (Brucker-Kley et al., 2013; Grimm & Chiasson, 2014; Holt et al., 2021; Locasto et al., 2011; Pfister, 2017), the responsibilities and burdens associated with handling the legacies of others (Brubaker et al., 2014; Odom et al., 2010), and speculative designs and critiques regarding the prolonging or imitation of the personhood of the deceased through digital means (Meese et al., 2015; Ohman & Floridi, 2018; Pitsillides, 2019; Wallace et al., 2018). Although the concept can be described using various terms, such as digital heritage, digital estate planning and digital remains, we will use the term digital legacy in order to align with the greater part of HCI research. However, where some digital research focusses on new

forms of deliberative inheritance and remembrance, such as the production and affordances of “technology heirlooms” (Odom et al., 2012) or social media memorials, our paper targets more naturally formed data and information legacies and the ways in which these might be directed by and managed according to user preferences. Massimi et al. (2011) identify four central stakeholder groups in the area digital legacy: mortals, the dying, the dead, and the bereaved. In this research, we have chosen to focus primarily on mortals and (indirectly) the dead, in an attempt to better understand the nature of views on appropriate behaviors toward and about the dead. However, our findings support a need for improved means of collaboration between these stakeholders – something identified as a missed opportunity in two recent reviews of HCI research on the topic (Albers et al., 2023; Doyle & Brubaker, 2023).

As technologies have developed, often focused entirely on their living users, some have called for the integration of mortality into the design of technology – a concept described by Massimi and Charise as *Thanatosensitivity* (Massimi & Charise, 2009). At present, such approaches are rare, but there are several notable instances of large online services that have developed functionality of this sort. Facebook, often cited as a service with growing numbers of deceased users (Ohman & Watson, 2019), introduced its *legacy contact* feature in 2015 (Brubaker & Callison-Burch, 2016; Gibbs, 2015). By nominating a person to act as their representative in the event of their death, Facebook users can enable the posthumous transfer of a measure of control over their profile, including the ability to update their profile picture, write a pinned post, download a copy of what they shared on Facebook and request the account be removed (Facebook, n.d.b; n.d.a). Facebook is one of the only major online services that allows for even partial assignment of rights following the death of its users, however even this is only the case in the event that the user has completed this process (Michels et al., 2019). Recent research has also indicated that many users who have done so may have expectations that do not fully align with the limited functionality that is actually offered (Gach & Brubaker, 2021) and there is limited clarity around how privacy settings go on to affect memorialization (Trevisan et al., 2023). Another relatively well-known design that factors in, if not death explicitly, at least the future expiry of its users is the Google Inactive Account Manager. Google’s approach is much more granular, allowing for certain data from a selection of Google’s services to be sent to certain named recipients (Google, n.d.). Unlike Facebook, there is no associated transfer of control, and rather than taking place upon notification and proof of the death of the user, the process will initiate following a defined period of user inactivity and unresponsiveness. Apple take yet another approach, with assigned legacy contacts requiring an access key generated by the user when selecting them as a contact (Apple, n.d.). Whilst it is encouraging that processes such as these have been developed, usage appears to remain low, with a recent poll indicating that as few as 3% of people in the United Kingdom (UK) have used such tools (STEP, 2022).

A natural disadvantage of built-in digital legacy functionality like that described above is that people sensitized to privacy after death may use many different services and would be required to understand and activate a separate legacy tool on each, all of which may differ in purpose and approach and have different requirements of the various parties involved. Doing so would be time-consuming, tedious, and cognitively demanding, and likely to create a burden for the individual(s) expected to navigate those legacy processes in order to carry out their wishes or access important information. Furthermore, there would be a need for constant review of functionalities and policies in order to maintain an effective plan, as well as an awareness of the legacy contact’s continued usage of the service in question. Another approach is to conduct digital legacy planning in a way that cuts across multiple services and data repositories. One available technology to do so is the password manager, which, by way of its usual operation, collects information about which services a user visits and the credentials that are used to access those services. Some popular password managers, such as LastPass (LastPass, n.d.) and BitWarden (BitWarden, n.d.), offer a means of transferring a copy of a user’s password vault to a pre-assigned user in the event of an “emergency,” using a dead man’s switch mechanism that can be initiated by their chosen emergency contact and can be canceled by themselves within a set period of time if they are living and well. However, the use of passwords to

control postmortem access in this way is also an imperfect solution, as it sits in a legal gray area (Michels et al., 2019), may allow for identity theft, affords no data granularity within services, and may become ineffective over time as security methods such as multi-factor authentication become commonplace and more advanced. Additionally, the use of password managers to transfer passwords may incur a premium tier subscription, which could become costly over many years, and relies on the exclusive use and longevity of the password manager service (Holt et al., 2021).

As an alternative to relying on legacy functionality within existing systems, some bespoke services for digital legacy planning have been produced in an attempt to fill a perceived market gap. These two approaches to digital legacy systems have been termed Integrated Digital Legacy Management Systems and Dedicated Digital Legacy Management Systems (Yamauchi et al., 2021). However, the market for dedicated systems has proven difficult to monetize, with services struggling to survive long enough to be able to deliver on their aims (Gulotta et al., 2016; Yamauchi et al., 2021). In the absence of established and widely used systems of either integrated or dedicated design, people who are interested in planning elements of their digital legacy may choose to implement a plan of their own design. Options in this regard include manually curated lists of used services and passwords, creation of hard drives containing important documents and data and deliberative sharing practices of nonsensitive, but valuable, information (Brucker-Kley et al., 2013; Holt et al., 2021; Kasket, 2019). In such cases, however, the user is required to be dedicated enough to the endeavor to spend considerable time and effort designing, implementing, and reviewing their plan. It is our contention that personal information management systems are well positioned to provide mechanisms for the enhancement of user agency in this respect.

2.4. Personal information management

Personal Information Management (PIM) tends to treat personal information as that which is in some way obtained, ordered and kept for future personal use by an individual (Jones et al., 2001; Lush, 2014), as opposed to the focus on personally identifiable data that is found in discourse on data privacy and legislation such as the GDPR. A considerable subset of PIM research can be placed under the label *file management*, in which the everyday usage of organizational constructs, particularly folders, is an important factor in how information is used in practice (Dinneen & Julien, 2020). PIM research has indicated that, despite many attempts to shift toward systems based on search or tagging functionality, users tend to prefer this directory-based structure when managing their personal data, and that they do so in ways that are highly individual (Bergman & Whittaker, 2016). Bergman et al. (2003) proposed a set of principles collectively named the *user subjective approach*, in which this individuality is reinforced by designing PIM systems to promote information according to subjective value, present information related by topic together, and keep the information within the contexts in which it was originally accessed. A key principle in traditional information management of this sort is that the accessor is expected to be the same person who originally organized the information, and that their primary aim is “keeping found things found” (Jones et al., 2001). Increasingly, however, this is becoming problematic, as shared spaces are becoming common and users are engaging in Group Information Management (GIM) environments in which the finder is not necessarily the organizer (Lutters et al., 2007). Within GIM systems, users are required to navigate additional data privacy and organizational complications and must organize and curate data in a way that can be expected to make sense to other users (Markus, 2001). Early research into GIM systems by Berlin et al. (1993) identified difficulties caused by differences between personal styles of data management, and detailed analyses of file retrieval suggest that failure rate and retrieval time are much higher in GIM environments than PIM environments (Bergman et al., 2014). Furthermore, the quantity of information generated is becoming difficult to manage manually, and users are turning to newer technological methods of information retrieval (Bergman et al., 2022). As the quantity and complexity

of data increases, there is a growing need to consider information longitudinally, including how users can be supported in decisions to keep or discard data and how to present information differently over time (Gulotta et al., 2015; Khan et al., 2018; Vitale et al., 2019, 2020). Research has suggested that long-term management of personal files is difficult, with users tending to be overwhelmed by the quantity of files and data and often deferring evaluation due to an inability to predict their future usefulness (Whittaker & Hirschberg, 2001; Whittaker et al., 2010). Boardman and Sasse (2004) also outlined the difficulties of managing large collections, identifying that approaches to the problem differed not only between individuals, but also that individuals each tended to employ multiple strategies, and that PIM solutions were required to support that variety of approaches whilst not penalizing those who chose not to conduct such organization.

We argue that postmortem data access represents a particular context of information management in which both curated personal information and data trails of a more passive and opaque nature have the potential to later become relevant at a group level, depending on the stated preferences of the individual and actions of their survivors. Failure to account for this context produces a risk that well-meaning loved ones of deceased users, seeking to act in accordance with their digital legacy and postmortem privacy wishes by retrieving certain valuable information, will find themselves operating within unfamiliar personal information environments that they struggle to navigate appropriately or effectively. In this research, we sought to clarify and evidence the complexity and contextuality of postmortem data access behaviors. By doing so, we hoped to elucidate this problem and produce implications for the design of digital legacy management systems or integration of digital legacy functionality.

3. Research design

3.1. Research aims, objectives and approach

We believe that the complexity of the problem of appropriate postmortem data access goes beyond dichotomies of public against private, or preservation against deletion. Basing our approach loosely on some of the factors outlined within Contextual Integrity (Nissenbaum, 2004), we aimed to take a deeper look at how nuances in postmortem data flows might affect judgments of appropriateness. We wished to consider, given an assumption that no preferences are specified before death, how different individuals interpret the appropriateness of postmortem data access when the context of that access is modified. In doing so, we wished to explore the social acceptability, from the point of view of the data subject, of different forms of postmortem personal privacy intrusion as they may currently occur.

Our primary objectives for the research follow.

- (1) In a systematic way, examine the extent to which contextual factors impact evaluations of appropriateness of data access during life and after death.
- (2) Explore some of the rationales, experiences and emotions associated with such evaluations and any observed changes in response to context.
- (3) Examine the extent to which postmortem privacy and digital legacy planning behaviors correspond with these responses, in order to further examine the concept of a posthumous privacy paradox.

In two closely related studies, we employed scenarios to describe different forms of data access during life and after death, seeking to gauge normative views on these behaviors and demonstrate the effect of vital status as a contextual factor. Both studies were conducted entirely with residents of the UK.

3.2. Study one

In Study 1, conducted in December of 2020, we used an online questionnaire to gather responses from a sample of the research population to a series of scenarios representing unauthorized data flows. We also gathered information about their evaluations of the importance of privacy and postmortem privacy more generally, as well as their engagement with legacy planning behaviors and tools.

3.2.1. Participants

Participants were recruited using prolific.co, a paid participant recruitment solution, which enabled us to recruit a sample of UK residents with varied age and suitably balanced gender ratio. A Call for Participation invited participants to join “a study about privacy preferences” that involved responding to scenarios that “will require you to think about or imagine things that might happen after you die.” Participants were paid an hourly rate of £10 per hour, calculated to £2 per participant according to the median time taken (Approximately 12 minutes). Responses were screened for quality using several attention check questions throughout the questionnaire. In total, 108 participant responses were accepted, with an even split between male and female and diverse in age ($M = 45.12$, $Mdn = 51$, $Range = 19-76$, $SD = 15.07$).

3.2.2. Method and procedure

In the main task of the questionnaire, participants were asked to respond to a series of 12 scenarios, each of which was near identical but differing across three key contextual factors, namely who the accessor is, what the data type accessed is, and whether the access is described as taking place during life or after death. The described usage of the data also varied in order to be consistent with the data type. An example scenario is as follows (relevant contextual factors underlined):

After you have died and without your permission, a close friend or family member gains access to your primary messaging application and reads through conversations you have had with other people.

The scenarios were presented in three blocks, each of which represented one of three types of data: *private messaging*, *digital files*, and *location data*. The data types were chosen as broad examples of common data that might elicit different evaluations of privacy, value, and usefulness. These blocks made up sections of the questionnaire, and the order of those sections was randomized. Within each block were four scenarios, varying across two dimensions: the accessor of the data was described as either a *close friend or family member* or by a *company or organisation* (to approximate a close and distant relationship with the accessor), and access was described as taking place *during everyday life* or *after you have died* (to represent vital status). The order of these scenarios was randomized within each block.

For each scenario, participants answered six seven-point Likert items, presented in the same order for each scenario. These examined to what extent the participant agreed with the following:

- “The information access described above is appropriate”
- “It was easy to decide how appropriate this information access is”
- “This type of information access is likely to happen to some people”
- “This type of information access is likely to happen to me”
- “I would give permission for this information access, if asked in advance”
- “It was easy to decide whether I would give permission for this”

The questionnaire also featured a section that asked some more general self-reflection on the value of privacy and postmortem privacy, and personal behaviors regarding this (shown in [Figure 1](#)). This section was presented either before or after the main task, in order to counter-balance priming

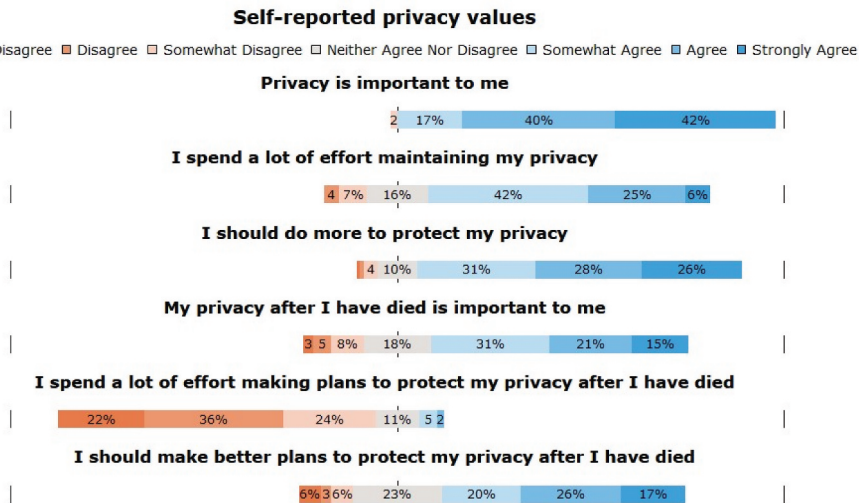


Figure 1. Responses to overall evaluations of privacy and postmortem privacy indicate a lack of action relating to postmortem privacy despite wide agreement that it is important.

effects. Finally, we asked participants to identify their engagement with a selection of legacy planning behaviors, in order to better understand the prevalence of currently available options. These are shown in [Table 2](#) and include legal actions, integrated digital legacy management systems and other available planning behaviors. We also provided a free-text space in order for participants to highlight techniques or services that we had overlooked.

The Study One data were analyzed using descriptive and inferential statistics. Given that our response data was not distributed normally, we judged that our data set fails the assumptions of parametric testing, and in our findings section we report on non-parametric analysis. To do so, we used the Aligned Rank Transform ANOVA (ART), which is capable of examining interaction effects within non-parametric datasets (Wobbrock et al., 2011).

3.3. Study two

In Study Two, conducted in November 2021, we sought to gain qualitative insights and individual reflections on the subject matter explored in Study One. Whilst our questionnaire explored the effects of contextual factors in a systematic way, Study Two captured individual perspectives more idiographically, focussing on the reasoning and feelings that were associated with evaluations of unauthorized postmortem data access. Given the comparative depth of consideration in this study compared to the first, it was not feasible to address all elements that had been addressed in Study One. As such, we chose to focus on judgments of appropriateness and limit the scenarios to access by a friend or family member, which had been the scenarios in which there was a notable difference between access during life and after death.

3.3.1. Participants

In total, the Study Two data consists of interviews with a new sample of 12 participants, consisting of five female and seven male and with a mean age of 58 years. All were UK residents, eight from the Northeast region, and had been recruited via Voice, a community of members of the UK public who wish to contribute to research and innovation. A new sample was used in order to capture initial reflections to the questions and scenarios utilized and avoid any priming effects of taking part in the survey reported in Study One. Participants were selected from a shortlist in order to ensure a spread

Table 1. Study two sample demographics.

Participant	Region	Gender	Age	Ethnicity
Olivia	North East England	Female	25	White British
Hassan	Central Scotland	Male	27	Pakistani
Leanne	South Wales	Female	36	White British
Mark	North East England	Male	47	White British
Susan	South West England	Female	58	White British
Michael	North East England	Male	60	White British
Suresh	London	Male	61	Indian
Andrea	North East England	Female	61	White British
Richard	North East England	Male	68	White European
Robert	North East England	Male	77	White British
Shirley	North East England	Female	81	White British
Charles	North East England	Male	93	White British

Table 2. Self-reported engagement with selected behaviors that may form part of a digital legacy plan.

	Yes	No	N/A	I don't know what this is	Prefer not to say
I have a will	29.6%	68.5%	0%	0.9%	0.9%
My will contains instructions relating to my digital belongings	0.9%	26.9%	70.4%	0%	1.9%
I have left other instructions relating to my digital belongings	5.6%	82.4%	10.2%	0.9%	0.9%
I have set up Facebook's Legacy Contact feature	4.6%	64.8%	13.8%	16.7%	0%
I have used Google's Inactive Account Manager feature	1.9%	71.3%	5.6%	20.4%	0.9%
I have put important files onto a USB stick, hard drive, or other form of device so that others can access them in the event of my death	19.4%	76.9%	1.9%	1.9%	0%
I often write my passwords down somewhere	25.9%	71.3%	0%	0%	2.8%
I often save my passwords in my web browser	52.8%	43.5%	1.9%	0%	2.8%
I use a password manager	26.9%	70.4%	0%	0.9%	1.9%
I have set up an Emergency Contact to be able to access my password vault	8.3%	41.7%	45.4%	1.9%	2.8%

of ages. Nine participants self-reported as White British. No participants withdrew from the study; however, we did exclude two additional interviews from the data set prior to analysis due to poor engagement with the interview (including multitasking, unresponsiveness, repeatedly leaving the teleconference) and technical difficulties. Based on prior research suggesting that data saturation typically occurs within the first 12 interviews, we judged the final sample to be appropriate (Guest et al., 2006). All participants were compensated with a £20 shopping voucher, including those whose interviews were not analyzed. Table 1 shows the participant demographics alongside their pseudonyms, which were chosen to align with age, gender, and ethnicity.

3.3.2. Method and procedure

Study Two interviews were semi-structured and conducted remotely via Zoom teleconference. Each interview was preceded by a short online questionnaire, identical to the basic privacy values section used in Study One; participants were asked at interview to elaborate on their answers to those questions, before being presented with a small set of data access scenarios selected from those used in Study One. During this part, the data accessors were always described as “a close friend or family member,” and the *during life* scenario was always presented immediately before the *after you have died* scenario in order to allow the conversation to naturally focus on any differences between during life and after death access. Participants were additionally asked to imagine and discuss access to data in the long-term future, such as by a descendent or historian.

We conducted a Reflexive Thematic Analysis of these interviews, following Braun and Clarke (Braun & Clarke, 2013). This analysis was primarily carried out by the lead author with the support of Quirkos, a computer-assisted qualitative data analysis software tool. This process involved familiarization with the data through repeated reading of the transcripts, before carrying out data-led coding and iterative grouping and regrouping of those codes. Codes and groups of codes were

organized into hierarchical structures; for example, “the wishes of the deceased should be acted on” and “confidence in handling others’ estates is empowering” are codes that were grouped under the broader code “navigating deaths of others appropriately”. This process involved sense-checking with the wider research team and resulted in the formation of a small selection of candidate themes, which we have organized into the findings that are presented in this paper. For example, the codes given above ultimately formed part of the theme *Mutual Responsibility*. As the presented findings represent those sections of the analysis that pertain most directly to the study aims and objectives, which are theory-led, we characterize our analysis as a combination of inductive and deductive approaches.

3.4. Ethical review

Both stages of the research were designed to minimize risks to the wellbeing of those involved. We identified that contemplations of death and dying are potentially distressing to participants and ensured that all advertisements, consent processes and instructions were explicit about the topic of the research. Informed consent was gathered for both studies, with additional verbal consent also confirmed at the beginning of the interviews, and both stages also ended with a clear debrief of the purpose of the study. All participants were made aware on multiple occasions that they could withdraw at any point. For Study Two, participants were informed that the interview could also be paused, in the event that they became upset but preferred not to withdraw. Interviews held over teleconference were preceded by a check that participants were in a comfortable and private place, could see and hear well, understood they were to be recorded, and were confident in their use of the teleconferencing software. All research conducted was designed to meet the ethical and data collection and processing standards of the lead author’s institution and was formally approved by their Research Ethics Committee as such with references 8531/2020 (Study One) and 21–022-HOL (Study Two).

4. Findings

4.1. Study one

4.1.1. Overall privacy and post-mortem privacy evaluations and legacy planning characteristics

Figure 1 shows the distribution of the Likert responses for items relating to overall privacy values, and we will report medians and interquartile ranges where the Likert responses have been transposed to numbers from one to seven, and where one represents Strongly Disagree and seven represents Strongly Agree. All statistical findings presented relate to a sample size of $N = 108$. Almost all (98%) of participants agreed at least somewhat that privacy is important to them ($Mdn = 6$, $IQR = 1$). Despite 73% of participants indicating that they already spend a lot of effort maintaining their privacy ($Mdn = 5$, $IQR = 2$), 84% reported that they should do more to protect their privacy ($Mdn = 6$, $IQR = 2$) – a result that we interpret as reflecting the difficulties associated with maintaining personal privacy. A significantly smaller majority of 67% (as tested using the Wilcoxon Signed Rank Test, $Z = 7.387$, $p < .001$) reported that privacy after death is important ($Mdn = 5$, $IQR = 2$), with fewer exhibiting strong agreement and 18% opting for “neither agree nor disagree,” compared with 0% for the general privacy question. A similar distribution is seen for responses to whether or not participants should make better plans to protect privacy after death ($Mdn = 5$, $IQR = 2$), suggesting that those who see importance in postmortem privacy also see their own plans as lacking. This is supported by the strikingly different response to the self-reported effort spent making plans to protect postmortem privacy ($Mdn = 2$, $IQR = 1$), with a strong majority disagreeing that they spend a lot of effort doing so. A Wilcoxon Signed Rank Test shows significantly reduced reported effort spent protecting postmortem privacy compared to lifetime privacy ($Z = 8.527$, $P < .001$). These findings support existing research identifying a postmortem privacy paradox – the phenomenon of individuals expressing value in postmortem privacy but not acting to protect it (Holt et al., 2021; Morse & Birnhack, 2020).

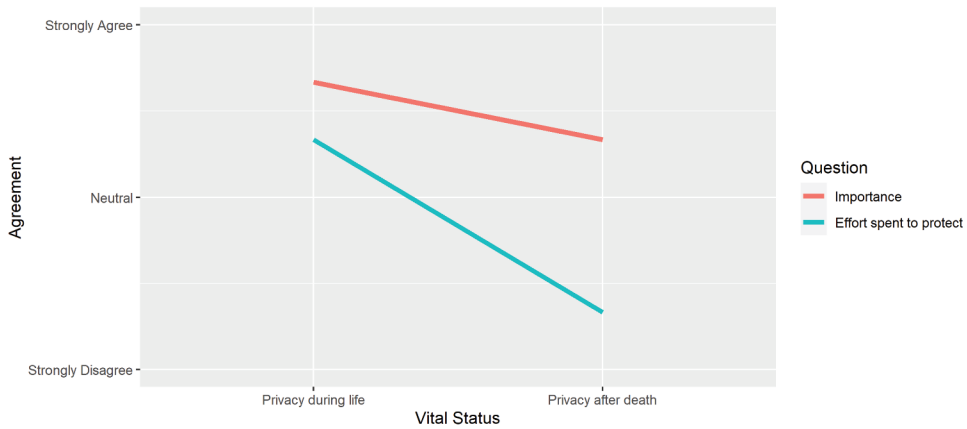


Figure 2. Median responses evaluating the importance of privacy and the effort spent protecting that privacy, shown separately for privacy during life and privacy after death.

Further, they appear to show a more pronounced gap between reported intent and effort spent in the case of postmortem privacy than for overall privacy, as illustrated in Figure 2.

Table 2 shows the numbers and proportion of participants who reported engaging with the selected behaviors that may form part of digital legacy planning or be an important factor in the handling of a digital estate. For this group of questions, there was minimal engagement with any activity specifically relating to digital legacy planning. At 19.4%, creating a USB stick or other hardware device with important files was the most commonly used technique for digital legacy planning. Use of platform-specific digital legacy functionality for Facebook and Google was very low, at 4.6% and 1.8% respectively.

In addition to these direct questions, an open ended free-text question was offered, in which participants could report unmentioned techniques that they have personally employed. No participants reported using a Dedicated Digital Legacy Management System nor any unmentioned legacy process integrated within a service.

4.1.2. Appropriateness and permission

Figure 3 shows the responses to the Likert item collecting views on appropriateness for each of the 12 scenarios described. There are a number of notable aspects to these results:

- (1) There is a clearly visible positive change in the appropriateness of a friend or family member accessing data without permission when that access takes place after death, and no corresponding change in appropriateness if the entity accessing the data without permission is a company/organization. Analysis of Variance of Aligned Rank Transformed Data shows a significant difference between appropriateness of data access in life compared with death ($F = 132.404$, $P < .001$), and a significant interaction in this effect with the accessor ($F = 69.528$, $P < .001$). This finding suggests that for those who report that postmortem access is appropriate even without permission, this appropriateness remains dependent on who the accessor is. The fact that an overwhelming majority considers unauthorized postmortem data access by a company or organization to be inappropriate further implies the existence of social norms that support some degree of continued respect for privacy after death.
- (2) The appropriateness for friend/family members to access data after death is not consistent across the three types of data presented in the scenarios. For digital files, approximately half

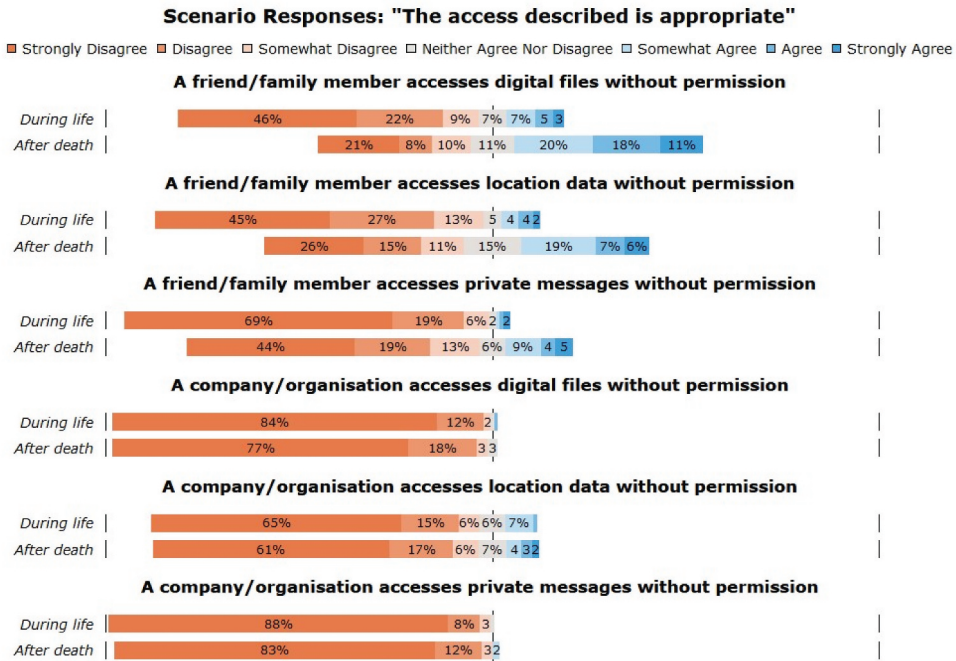


Figure 3. Percentage responses for different strengths of agreement that “the access described is appropriate” for each scenario.

agreed to some extent that the access is appropriate ($Mdn = 4$, $IQR = 4$), compared to only 18% for private messaging ($Mdn = 2$, $IQR = 2$). There was a significant difference in appropriateness according to data type ($F = 77.320$, $P < .001$), as well as a significant interaction between data type and vital status ($F = 25.592$, $P < .001$) and a significant three-way interaction between data type, vital status, and accessor ($F = 23.130$, $P < .001$). These interactions are illustrated in Figure 4, which shows changes in mean responses between the “during everyday life” and “after you have died” scenarios across data type.

- (3) The change in appropriateness for friend/family members is not exhibited by all participants, and participants show strong opposing views in the after-death scenarios, particularly in relation to digital files. Figure 5 shows individual changes in appropriateness for these scenarios.

As shown in Figure 6, willingness to give permission can also be seen to increase for the after-death scenarios when the accessor is a family member or friend, but not when the accessor is a company or organization. We found significant differences in willingness to give permission according to vital status ($F = 44.8832$, $P < .001$), data type ($F = 79.913$, $P < .001$) and accessor ($F = 441.867$, $P < .001$). As with appropriateness, we also found significant interactions between all independent variables (Data Type * Vital Status: $F = 5.876$, $P < .005$; Data Type * Accessor: $F = 41.797$, $P < .001$; Vital Status * Accessor: $F = 69.528$, $P < .001$; Data Type * Vital Status * Accessor: $F = 7.1402$, $P < .001$). With 70% agreeing that they would give permission for access to digital files ($Mdn = 5$, $IQR = 2$), this result suggests that a majority of our sample possess at least some form of digital entity for which they would consider it suitable to arrange postmortem access for their loved ones.

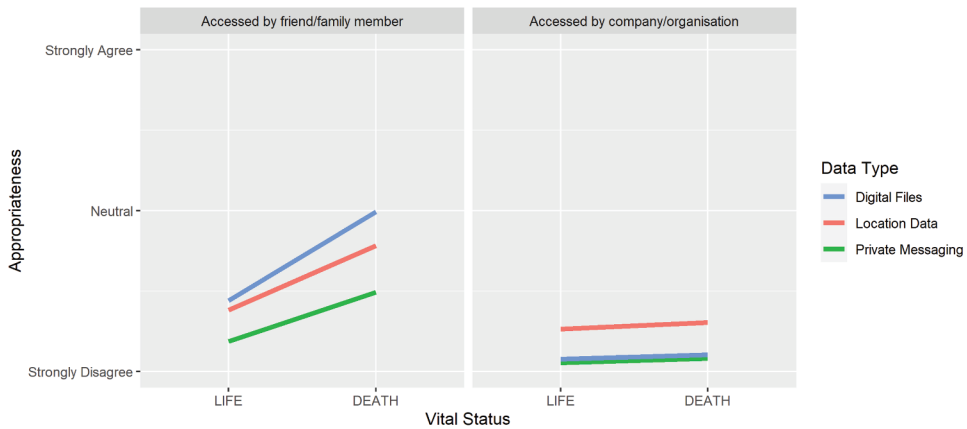


Figure 4. Means of judgments of appropriateness show interaction between vital status, data type and accessor.

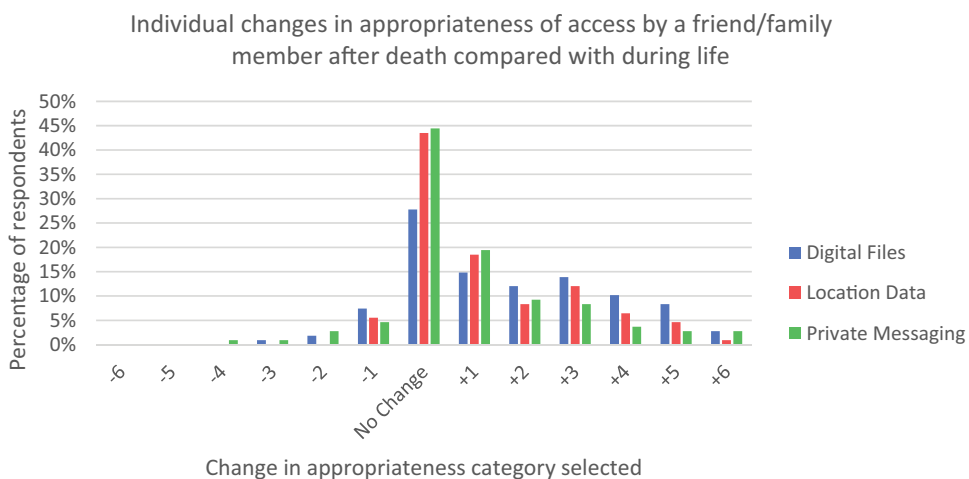


Figure 5. Individual changes in appropriateness responses when considering after death data access with the same during life. E.G. A change from agree to strongly agree would be represented by + 1. For friend/family access scenarios, many participants scored after death access as more appropriate. However, between 28% and 44% scored before and after death equally.

4.1.3. Ease of answering and scenario likelihood

For questions relating to appropriateness and permission, as described above, we collected Likert scores for the ease with which those questions were answered. The majority of participants reported that the tasks of deciding appropriateness and deciding whether or not to give permission were easy for all 12 scenarios, with the proportion of participants at least somewhat agreeing that judging appropriateness or permission “was easy” never going below 82% across all 24 of these questions. When combining this result with the evidence that these participants broadly do not engage well with the task of digital legacy planning, we see an indication that it may not be the decision-making element of the process that is likely to be the cause.

For each scenario, participants provided an indication of its likelihood of happening to “some people” and also to themselves personally. The agreement that the scenarios were likely to happen to some people was high across all scenarios, with at least 69% agreeing to some extent in all cases. The most likely scenarios were those in which a friend or family member accesses digital files (Mdn = 6, IQR = 2) or private messaging (Mdn = 6, IQR = 1) after death, at 88%. In most cases,

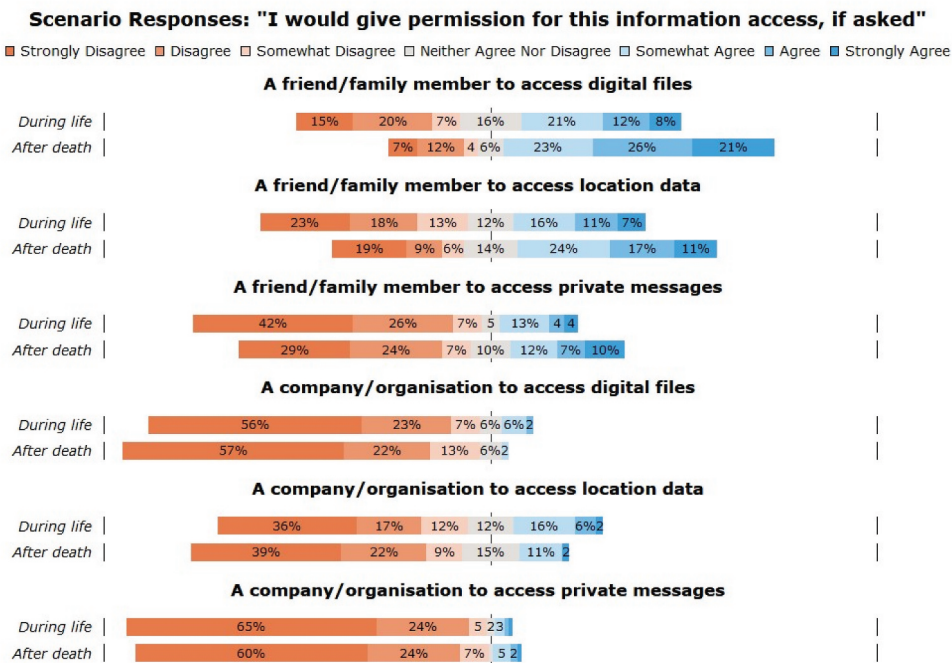


Figure 6. Percentage responses for different strengths of agreement that "I would give permission for this information access, if asked in advance" for each scenario.

likelihood of happening to some people did not vary much between life and death except in the case of a company or organization accessing location data, which 87% agreed was likely during life (Mdn = 6, IQR = 2) and 69% (the lowest across the scenarios) agreed was likely after death (Mdn = 5, IQR = 2). This difference may be a reflection that companies are perceived to have an interest in current rather than historic location data information.

The perceived likelihood of the scenarios happening to the participants themselves was lower than the perceived likelihood of happening to others and with a greater incidence of neutral answers. The most-likely scenario by a clear margin is a friend/family member accessing digital files after death – at 66% agreement (Mdn = 5, IQR = 2), almost twice as many participants view this scenario as likely compared than the same person accessing location data (Mdn = 4, IQR = 2) or private messaging (Mdn = 4, IQR = 2) after death. However, across all three data types, a friend or family member accessing after death was seen as more likely than the same person accessing during life. This finding implies that participants perceive a stronger rationale for unauthorized access of data by a close friend or family member after death compared with during everyday life. Figure 7 shows the case of digital files in more detail, with the likelihood of the friend or family access scenarios happening to others shown alongside that of happening to themselves.

4.1.4. Study one findings summary

Our findings from this survey can be summarized as follows:

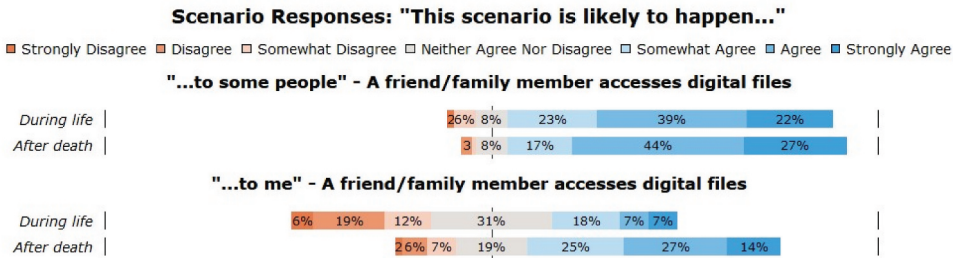


Figure 7. Participant responses to questions about the likelihood of unauthorised access to digital files.

- Despite reporting that postmortem privacy is important, participants reported not spending much effort planning to protect it and largely did not report using any tools for digital legacy planning.
- Appropriateness of unauthorized data access after death is individual and contextual, varying across participants and depending on the type of data accessed and who is accessing it. It was widely considered inappropriate for companies or organizations to access postmortem data without permission, suggesting a continuation of some degree of respect for privacy after death, although it was unclear if this was perceived to be for the benefit of the deceased or for others.
- The proportion who would give permission for the described data access varied across the same dimensions in a similar fashion. The proportion of participants who said they would give permission was greater than the proportion who found such access without permission to be appropriate.
- Participants found the given scenarios to be realistic, but weren't sure they would be affected personally. However, a majority saw their friends/family attempting to access their digital files after death to be likely.

4.2. Study two

This section provides an overview of our thematic analysis, which we present as four themes: Projection of Data Values, Conflicts of Self-interest and Altruism, Mutual Responsibility and Navigating Privacy Boundaries in Good Faith.

4.2.1. Theme 1: Projection of Data Values

With this theme, we describe elements relating to participants' projections of both the future of their data and the perceived value of certain data for other people. We present findings that highlight the ways that changing and unpredictable contexts could impact valuations of data and data privacy.

Across the three types of data (digital files, location data and private messaging), the most natural and intuitive for participants to associate with value for others was digital files. Photographs are commonly inherited and often valued items, and this is reflected in Richard's experience:

When my parents died, quite a number of years ago, we didn't have the technology of today, we didn't have, you know, many thousands of photographs, it was a straight-forward thing. And when they died [...] the photographs in the album – I've still got them, they're in the attic. They're probably stuck together and what have you. But they thought that they were something they wanted to remember from their life, therefore, you know, expecting I think that I've kept them. And shortly after their deaths we sat down as a family, and we went through them. And I've kept them, and I'd like to think that when I go, because most of the photographs there are of me, that someone will want to have a look at them. – Richard

In Richard's case, the value of the photos appears to be shared between the deceased and the inheritor. In recognition of the importance of the photos to his parents, he describes a viewing of them as a family activity of remembrance – that they represented valued memories of his parents

seems to add value for him. In turn, their continued value after his own death is shared, with the idea that others might go on to find value in them itself having value to him. A younger participant, Olivia, identified her digital photos as her main source of sentimental value:

I am really sentimental. So, yeah, I would probably [...] just give them access to like my hard drive with like all my millions of photos on them all, and [...] I would want people to be able to look back or remember me by certain things. – Olivia

For Olivia, any curation activities are left to the discretion of the recipient, which may be a result of the anticipated quantity of photos. The potential impact of such organizational tasks was highlighted by Charles, who described family photos as *“important and interesting for a time”*, but ultimately concluded that this interest is limited, and *“you can only look at X number in any one day, even if you sit in front of a screen and look at them continuously”*. For these reasons, Charles spoke of information being relevant and valuable within particular temporal contexts, as in the case of his location whilst working, which he would have been open to sharing at the time as he *“felt other people should know what I’m doing.”* Beyond a certain point, he felt that *“treasures”* were subject to expiry and that *“you have to decide how long they are a treasure”*. For some participants, there was a desire to preserve value. Robert spoke of his experience digitizing old family photos:

They’re in both [...] physical and digital form because I went through all the old family photographs that I could find and [...] I digitised them and sent discs to my two daughters, partly as a backup and partly because they’re genuinely interested [...] And before, before my mother died, I actually got her to go through the photographs and write on the back who they were and, if relevant, where they were. Because we have some photographs from our own sort of teens and 20 age band, and we don’t know some of the people on the photographs. Which is quite frightening, I think. – Robert

Robert’s comments on the importance of identification of the subjects of the photos suggest that they have value not only as a means of remembering, but also as a source of information. In his case, those annotations are *“not kept together”* with the digital photos, suggesting that supporting information has been filtered out through the digitization process, leaving the photographs as the core artifacts that are passed digitally to his daughters and potentially onwards to further generations. In this context, location data, which he otherwise described as *“boring”*, may have latent value that becomes evident when used in combination with photos.

In order to explore the perceived future of data on a more long-term scale, participants were asked to reflect on their feelings about access to and usage of their data many years in the future, such as by a descendent or social historian. For all participants except Charles and Suresh, this scenario produced an enthusiastic response, such as from Richard:

Under that scenario, I would be extremely happy, for that. From a historical point of view. Someone looking at my life after I was dead, that they’d be interested in me, as a living human being to see what I’ve been doing, no problem. 50 years down the line, no problem whatsoever for my location data [...] in 50 years’ time, people won’t really remember, unless they can access things like this, and maybe things like transport infrastructure and social awareness and everything else, like that would help, never thought about that before, but yeah. – Richard

Richard’s reaction illustrates the transformation of mundane data when considered from a new perspective or put to unanticipated use. When presented with the scenario in which someone close to him hypothetically accessed his location data during life, he had responded that they should *“get a life”*, yet access to the same data 50 years or more later appeared to him not only to be acceptable, but also to be of societal benefit. Likewise, Michael described his own data as uninteresting on an individual level, but recognized that it could be more mundane elements of life that go on to have value in the long term:

People think that history is all about big battles, famous people who built houses, and it's not, it's social history that's far more, you know, interesting from a local point of view of how everyday lives were led. And I think you know hundred years' time I'm sure they'd find it a bit boring, my life, but you know I wouldn't, from a social historian point of view, you know, I'd be quite happy for them to, to look at it. – Michael

Michael was not alone in seeing in this hypothetical scenario a reflection of his own interests and values: Hassan, Leanne, and Shirley also each referred directly to their own interests in genealogy and social history when prompted to consider the appropriateness of a descendent perusing their personal data long after their death. Shirley, for example, related to the value that is to be found when learning of the location of an ancestor when working on her family tree, remarking that *“when I do find out where they were at certain times, I’m, I’m really pleased that there’s information about them”*. Hassan, though largely in favor of postmortem privacy, saw value in the possibility of using modern technology to see ancestors *“properly”* and stated that *“if a descendent of mine had an opportunity to look at my life, I think I’d be open to that.”* He further described this nature of postmortem data access in a manner that suggests a transformation of focus; where previously consideration of these data would have been fixated on him as the data subject, in this scenario it *“might be ok”* as the access would be *“about seeing life through my eyes”*. Susan remarked that she did not see a loved one perusing her location data as part of their grief process to be *“healthy”* and would be *“worried about their sanity”*, but found that distant-future access *“changes the perspective”*:

I wouldn't have a problem with that, because I think with the passage of time there it changes the perspective so yeah [...] suddenly that flips over to being for a different completely different purpose, and I think that's different. – Susan

In contrast, Charles and Suresh each spoke on this in terms of practical use and questioned excessive focus on looking back on the dead, with Suresh arguing that *“people get so carried away with family trees and all that, why is that important unless it is for medical reasons?”* Mark, though mostly optimistic on the matter, had some reservations that the changing nature of societal values may be problematic with respect to long-term data. He referred to his late father, who he said would have *“been appalled”* at the way that he and others shared private details on social media. In reference to his own historical data, he wondered whether what he has said and done might be misrepresented or judged out of context by future generations:

It may be about it being judged in a way in the future, which doesn't reflect the time you lived in. So, what I'm thinking about here is, you know all this thing about slavery, and that, statues. And people being judged by today's values. And it doesn't make it any more right what they did with slavery, but it was a different time, it's missing context. – Mark

Underlying each of these responses is a personal interpretation of the potential consequences of a postmortem record of the participants' personal data. In considering their own future data, they must project the future value, interpretation, and usage of the data, and they do so according to their own experiences and worldview.

4.2.2. Theme 2: Conflicts of Self-Interest and Altruism

This theme describes the balancing of participants' own needs and wishes against those of others. We find that preferences for both privacy and openness are typically expressed in terms of effects on other people, but still relate to the individual's own sensibilities.

Despite evaluating data in terms of their own values, some participants (including Olivia, Leanne, Michael, Richard, Shirley and Charles) dismissed or diminished the notion of postmortem events affecting them personally, professing instead that any preferences given were for the benefit of their loved ones or for society more broadly. An inner conflict about the rationality of posthumous self-interest surfaced frequently in discussions of invasive access to postmortem data, as is seen in the following extract from Leanne:

It's a difficult one, because obviously you're not here anymore are you, so it was a bit like well wouldn't, wouldn't care anyway because I wouldn't be here. But at the same time, if I was here, I would be concerned if, you know, like there was a breach of I don't know some really like medical something you know, medical information or, you know something quite sensitive, you know that got out. I wouldn't be happy, you know, even if I wasn't here anymore. – Leanne

These participants grappled with contradictory viewpoints, characterizing their future posthumous selves as disinterested only to later express a preference (often in response to a scenario) for certain events to take place or not take place after their deaths.

You know, I have a philosophy that when you're dead you're dead. Doesn't matter to you anymore. – Richard

I think that when you die, you want people to look at you in the better light, you know. – Richard

In consideration of her privacy after death, Shirley acknowledged that, when dead, she will not be in a position to be harmed. However, this did not prevent her from characterizing privacy invasions after death as negative events.

And I think again it's, I would consider it erm, I would consider a friend who did this, to whom I hadn't said, you know, you can read all my stuff when I'm gone. I would feel if, it wasn't a good thing that they've done, but I'm dead aren't I, I can't have any feelings. – Shirley

A similar stance is assumed by Charles, who questions the appropriateness of these kinds of invasion without basing his argument directly on the harms suffered by the dead.

Charles: I would be worried, now, that somebody might want to [access my private data] after I'm dead, but I don't think I can do much about it.

Interviewer: I see, so, so you do feel that there is still, there is still a privacy issue there?

Charles: Maybe, but to a degree. I have very mixed feelings of how much one should know about dead people.

In this, Charles suggests a degree of powerlessness about what others might do after his death. A similar sentiment is expressed by Olivia, who identified a concern with postmortem access mainly because she wouldn't want the accessor to be "*hurt*" or "*worried*", and the "*uncomfortable*" feeling when imagining them learning private information about her.

I mean it feels uncom- now thinking like, it's an uncomfortable feeling if I thought like oh imagine if somebody thought that about me my whole life and then, and then they thought I wasn't who I was, or I wasn't quite what they had in mind. It's kind of weird, I don't quite like that, but I guess, I couldn't do anything about it, could I? – Olivia

Likewise, Shirley indicated that, hypothetically, she might prefer for certain information to stay private to protect others from harm even though "*it wouldn't matter to me personally, whether they knew or didn't know*". This kind of preference for postmortem privacy for the sake of others was most evident in the case of Suresh, who was the only participant to argue for increased privacy after death (although he would later go on to argue for a transparent and controlled process for postmortem data access).

There will be a change at death and then it's probably going to be a more stringent requirement after I'm dead ... only because I want to protect my loved ones. Because, while I'm alive, I can then turn around and say to my children to my wife actually I don't have any problem if someone uses that. I don't know what the consequence will be after I'm dead, I don't want to put them through difficulty. - Suresh

His opinion had been instigated by an unpleasant experience in which he had been contacted during the night by the police, who had mistakenly identified an elderly and confused man for his own late father – an experience that "*generated all kinds of emotion into me because my father had passed away*". For him, this "*planted the seed*" that postmortem data should not be retained needlessly after death so that "*something like that doesn't happen to the people I leave behind when I'm gone*".

In our interviews, we also found examples of value in postmortem sharing of information, and likewise with some combination of self-interested and altruistic reasoning. Shirley, a keen writer for many years, described wanting “*to make sure that people have access*” to what she had written. She anticipated that the writing would have value to others, especially those parts that are linked most strongly with her life and her identity, and so its continued value is contingent on their interest. At the same time, she identified her own hope that they will be interested in the writing and in her life stories.

I also hope that they might be interested, I know that, I know that my sons are very interested. You know, in all that I write, and, but, and I say to them, sometimes [...] if there’s anything you want to ask me, you know, ask me. Because I’m always aware that I never asked my mother enough questions. That she would have answered if I’d asked, she wasn’t keeping them private. She didn’t always realise that the things that she could say were, were valuable. – Shirley

A similar comment is made by Andrea, who did not expect others to be interested in her own data yet notes that not asking for such information from her father was one of her “*biggest regrets*” and that it is “*sad*” that a generation can get “*forgotten, almost*”.

In her case, there is a benefit to the potential recipient of such information, as they are protected from experiencing the same feelings of regret. There is also an implied benefit to those who might be prevented from being forgotten. The value of being remembered was also a feature of discussion with several participants, perhaps most notably Mark, who spoke of his own future legacy in terms of the fact that he does not yet have children, and may not follow the typical pattern of one’s children being their primary legacy, or of passing on things of importance to one’s children. Instead, he spoke of impacting society more broadly, and the value of sharing information not only with immediate descendants, but with younger generations as a whole.

So, most people pass on the legacy through their children. And it’s the thought that if I don’t do that starting to dawn on us now. You know, where a lot of people I left school with have had families, some of them are grandparents and the amount of information [older people] have got. The amount of erm, stories and useful stuff they’ve got to share with society. Someone needs to like almost encourage them to share it. – Mark

Alongside his desire to leave his own legacy, Mark implies an overall loss for society when it fails to seek out and learn from the life experiences of older citizens. He can be seen to embrace the importance of such sharing in practice through the sharing of his father’s writing:

Mark: well [my father] did a lot of what my mate described [...] as haikus. And you know what they’re perfect for? They’re perfect for a tweet. I’ve started tweeting some of them out. And I’ve got some responses from professional writer people on Twitter, saying oh I like this ... so I think, as much as I’ve said he wouldn’t have agreed with us doing everything public, he was always seeking for a way to share his writing. – Mark

In this example, Mark is acting in the (posthumous) interests of his father, in his own interest in the sharing and celebration of something that he considers valuable, in recognition of the importance of leaving a legacy generally, and in the interests of all those who may find value in his father’s writing.

4.2.3. Theme 3: Mutual responsibility

With many participants reporting experiences of responsibility over the handling of deaths of others, this theme outlines the perceived responsibility of individuals to leave for their loved ones a tidy state of affairs and clarity of expectations.

One of the most prevalent rationales for a perceived need to make some form of digital legacy plan was in order to support the needs of those who would be likely to take on a position of responsibility in the event of their death. 10 out of 12 participants referred to deaths of others that had affected their stance on this matter, although not necessarily with reference to the digital

specifically, and most had played a direct role in handling the deaths of close family members such as parents, spouses, and children. As a result, they felt a responsibility to ensure that they leave a tidy state of affairs for others.

The only thing that concerns me today, in life, is that those have the, to sort things out, have the ability to sort that out in the way that they want to sort it out and not be confronted by lots of red tape – Richard

Younger participants Olivia, Hassan and Leanne seemed to have engaged little with planning for death in any capacity, whilst others exhibited evidence or intent of traditional estate planning but felt unprepared with respect to their digital assets.

I've got a file with some things that felt important in life. My memories are in [a] box, but a lot of what is in the last 10 or 15 years a lot of them are in here [gesturing to computer]. You forget about them, in the ether, and you just kind of have to, I don't know. I don't know. I suppose if it mattered so much we'd do something about it, wouldn't we? – Richard

Richard reached a conclusion that failure to act must represent lack of importance, however, he has not failed to prepare with respect to non-digital items, which suggests that it is difficulties associated with managing digital information that are truly the cause. An example of such difficulties is given by Michael, who, citing the needs of an executor, identified an approach that would require significant changes to his use of e-mail services:

I mean I've been an executor of wills before and, you've got to you know give people, you know, the right tools to be able to carry out your will. And if they've got a super locked email account, then, maybe, maybe, I've never given it much thought really, but maybe I need like two accounts, one that is sort of the business end of things, one is like personal emails that don't get opened, and you know, ever get seen because people don't know the password and don't, you know, look. I've never thought about it really. – Michael

Several participants voiced a need for a simple means of managing their digital estates in order to make things straight-forward for their loved ones. Mark sought a legal means to identify certain actions that should take place. Leanne identified that she would use processes similar to Facebook's *legacy contact* or an app that would “*take care of all these things*”. Robert also indicated a preference for some form of digital legacy management system:

I would love it to be made as easy as that so that you could just get a package that you could literally say right, you can't have that anymore, that's gone. And, obviously, that would be a legacy issue then for, for my family. – Robert

One of the most prevalent things that participants felt they could achieve through legacy planning was the provision of clarity. Susan, Shirley, Leanne, Suresh, Michael, Robert, Olivia, and Andrea each spoke of the importance of people knowing what their deceased loved ones would have wanted.

I lost my mother earlier in the year, and it has [...] heightened my awareness of the importance of how you can actually lighten the load, if things are left in relatively good order and your wishes have clearly been, um decisions have been made, rather than leaving it open to interpretation. It's, it's a lot easier if you've got it laid out that these are my wishes. – Susan

Some people might like to shut their eyes to the whole thing and say, well, I won't be here, you can do what you like, but, when people are told they have to do what they like it means that they've got to make the decisions. – Shirley

However, even assuming that individuals had a sufficient means of forming a workable digital legacy strategy and the motivation to do so, they still face the problem of identifying future uses of data, as highlighted in *Projections of Data Value*. This difficulty was inadvertently demonstrated by Suresh, who provided an example of someone who should not be able to access personal data and then corrected himself on discovering a circumstance under which he would deem their access suitable:

But then it should be limited to those to whom that message will be applicable it shouldn't be just openly. For example, you know, a local council officer accessing my personal data – no [...] I do not see why a councillor, unless the council is actually trying to see who am I, how can they trace my loved ones, if they're accessing that information so that they can find my family my, my loved ones, so that they can actually inform my loved ones who I am – if it's being used for that purpose I do not mind. – Suresh

In this example, Suresh initially considered access to this data by the council officer to be outside of the legitimate needs of their role, before reconsidering and conceding that attempts to discover personal information could be consistent with carrying out their role in good faith and in support of his interests. Our fourth and final theme addresses this notion of privacy intrusions undertaken in good faith.

4.2.4. Theme 4: navigating privacy boundaries in good faith

This theme reflects how the ambiguity of potential legitimate needs may make unauthorised post-mortem access more acceptable. We suggest that participants' evaluations largely depended on data access and usage being conducted in good faith, rather than inherent privacy or openness of data.

In considering unauthorized data access in life, all participants indicated that they would react negatively if they were to experience such intrusions by trusted friends and family members, ranging from disappointment to anger. Often, this was not a reaction to particular risks or secrecy associated with the data in question, but a matter of principle. For example, Richard remarked that *"I'm not a private person, but I think it's important that if I want to be private, if I want something to be private that I should have that right"*, Leanne felt that the accessor would have *"crossed a boundary"*, and Hassan identified an *"unwritten rule"* that *"you don't open anyone's letters, and you don't go through their messages"*. Breaching clearly established privacy boundaries was often spoken of as inconsistent with friendship. Furthermore, the closeness of the relationship with the accessor could be seen to affect the perceived strength of the wrongdoing, as in the case of Leanne, who remarked that she would *"probably feel more angry at a close friend or family member, because I'd know them, you know"*. In the event of such an intrusion, participants indicated that they would require an explanation, but struggled to see why, in life, the accessor could have good intent and not have attempted to acquire permission before accessing the information in question. Olivia, in considering access to location data, found that *"it makes you kind of think like, do they trust you, or like what, why, what's pushing them to do it."* For Richard, *"it's the fact that they're doing it without asking me, that's the only thing, you know, why are you so interested in what I've got?"*. Mark supposed that the access *"could just be to do with being nosy"*, but was also willing to consider the possibility that certain intrusions may be committed for *"good"* reasons:

I'm turning this scenario around and I'm thinking. Sometimes, it doesn't feel like it at the time, but a close friend or a family member could be trying to gain access to your messages because they're concerned about you. – Mark

Considering the same access after death, participants held a range of opinions, however typically those judgments depended on the perceived likelihood of the accessor having a sufficient reason to access that data. Participants identified some situations in which ideal standards of privacy may need to be compromised in order to serve a greater need. For example, an accepted data access need for some participants was for close loved ones to be able to access contacts in order to share important information. Robert described being uncomfortable with others accessing private messaging after his death, but concluded that access to such data was legitimately required, and hence acceptable, but only by certain individuals and for that given purpose:

No, I still don't particularly like that, I mean, I think. This is where, in my book, privacy extends beyond the grave [...] having said that they would probably want access to my email contacts, so they could tell people that they weren't going to get any more emails from me. But other than that. And you can't really give one

without the other. I don't think you can anyway. Certainly without, you couldn't without making it difficult. – Robert

Robert did not indicate that representatives should require explicit permission, only that appropriate access is limited to what is sincerely needed in order for them to conduct their duties. In contrast, Susan saw a similar need for access to this data, but still considered explicit permission to be required in order for that access to be appropriate:

I guess that it would be, if it's the family members that I've nominated that's absolutely fine, I've got no issue with that whatsoever, because they may be wanting they may be needing to do that, to make contact with certain individuals and it's quite important to me that, for example, there are people that I want to acknowledge [...] and I need to give some thought as to how that that's done and how that there's access to that because that that's, that's really, that's really important to me that, that acknowledgement [...] but, the "without your permission," that, that changes it again, back to the others – Susan

Susan remarked that, having given such permission, she would *"trust their judgment, because I don't think I can tie them too tightly, I either have complete trust or I don't."* Likewise, Robert said he trusted his representatives to act in his interests:

Ultimately, I have no control over that once, once I'm not no longer there unless I go back and haunt them. But, they know broadly what I would like, and you know, why wouldn't they follow it if they can – Robert

For Suresh, postmortem access to data should be conducted in a manner that is accountable to other living individuals. Having initially spoken of data privacy as needing to become more stringent after death, he later spoke in favor of a more systematic approach:

Yes, provided ... those individuals are also supervised, that that's the only reason they accessing that information, and they also inform the people who are going to be impacted that this is how they found out, so at least then they're doing it transparently. They don't do it under stealth. They're not doing it quietly, they're doing it transparently, they're declaring that they've done it, and people are okay with that, then I don't have any problem with that. So it's all about governance and assurance, I think. – Suresh

In Suresh's proposal, there remains a need for certain individuals or institutions that wield decision-making responsibilities regarding his data – in his words, those who *"supervise"* the access of private information. Charles likewise assigned "moral responsibility to decide what should be done" to "the people who are left with it in their hands." For Leanne, such a person would serve to limit privacy intrusions after death:

I think if it was, if I knew the person that was going to be doing it. And I'd agree to it, or even if I hadn't agreed to it, but it was just one person. Like my partner, for example, or my best friend or something like that, then it's a bit different because it's just one person. And you possibly know who it's going to be. But I think, no, no, you know it's not like an open invitation for people to go in and have a snoop around. – Leanne

In her case, privacy is considered to be ongoing, but certain intrusions *"for a reason"* are expected. A similar expectation is expressed by Michael, who referred to a precedent for such necessities in the handling of traditional estates and identified his likely representative as his executor, who will have a clearly established role that includes discovery and identification of financial assets. Likewise, Andrea spoke of *"whoever you put in your will as your next of kin"* as having responsibility, and remarked that *"I think mine would know that I wouldn't want photos put on the internet or something like that."* She specified that she would have no problem with her children accessing her files, but that *"brothers and cousins or whatever, I wouldn't want them looking through my personal photos."* Typically, participants spoke of parents, spouses, and children as their likely data stewards were they to die in the near future. However, from among even this small group of participants, there were those who did not

necessarily feel that their own situation aligned with this structure, including Charles and Mark.

This isn't the first time I've thought about the kind of questions you're asking me, this is constantly with me and strangely enough, out of four of my friends, three of them are my age, actually five, out of five of them four are my age, we haven't got kids, and we're unmarried. And ... we're all on the same kinda boat. And I think there's more and more people than you think, it used to be the thing. Like my mum and dad's generation, where the thing was you did marry. And you did have children and you had a family and then nearly everyone did that, and now, things have changed – Mark

For people who cannot easily identify natural candidates for the role of identifying and executing appropriate actions, it may not be sufficient to have faith that others will act on their behalf after death. For those who wish to plan their postmortem privacy and digital legacy, but cannot or do not wish to place decision-making responsibility on others, there remains an additional task of anticipating the future and exerting agency through more involved planning methods.

4.2.5. *Study two findings summary*

Key findings relating to each theme are summarized in [Table 3](#).

Table 3. Key qualitative findings, organized by theme.

T1 Projection of Data Values

- Files, especially photographs, were seen as likely to have particular post-mortem value. However, that value can diminish with time, excessive quantity and in the absence of supporting information.
- Some mundane data could accrue value with the passage of time, meaning that post-mortem access by others is more understandable and acceptable. However, such values are subjective and not universal, and participants required prompting in order to identify this value.
- Changing contexts could mean that data could be used or evaluated in ways that would not be pleasing to the individual and may tarnish their memory.

T2 Conflicts of Self-Interest and Altruism

- Many participants dismissed the notion of being harmed posthumously, yet seemed also to prefer certain post-mortem outcomes.
- Some held preferences for post-mortem privacy but did not feel they could act on them.
- Participants typically positioned the importance of death planning in terms of the effects on others, but this was used to justify both privacy and openness.
- Many still wished to promote some of their own values and interests, but they needed to be balanced against the needs of their survivors.

T3 Mutual Responsibility

- Most participants had experienced the responsibilities of handling deaths of others and felt a mutual responsibility to ease this burden on their survivors.
- Planning for the digital was perceived as difficult, especially given the difficulties of predicting future needs or uses of digital content and data.
- It was considered important to provide clarity of intent as well as information, so that survivors can know they are acting appropriately.

T4 Navigating Privacy Boundaries in Good Faith

- Participants' negative reactions to lifetime privacy intrusion scenarios were based on perceived boundaries and unwritten rules.
- Post-mortem intrusions were seen to have potential legitimate explanations, which, in some cases, softened reactions.
- Participants, if willing to provide post-mortem access, did not wish to be overly restrictive, instead wanting their representatives to use their own judgment and trusting them to act in good faith.
- However, not everyone has a suitable candidate to act in their interests or who is close enough to fill this role.

5. Discussion

5.1. Overview

This pair of studies aimed to evaluate how a person's hypothetical status as living or deceased impacts their assessments of others' access to their personal data, using unauthorized access scenarios to surface sensitivities. Our results suggest that for many people, there can be a positive change in the perceived appropriateness of such access after death, but a considerable portion (varying by scenario) see no such change or even a slight negative change. We further aimed to assess the extent to which contextual factors may play a part in such evaluations, finding that judgments of appropriateness and willingness to give permission varied significantly according to the type of data and the accessor. Whilst prior research has suggested individual differences in preferences for different types of data and online accounts in terms of whether they should be transmitted or deleted (Grimm & Chiasson, 2014; Massimi & Baecker, 2010; Morse & Birnhack, 2020; Nakagawa & Orita, 2022), we understand at time of writing that ours is the first to consider the appropriateness of such access explicitly without permission or to consider postmortem privacy violations in direct comparison with lifetime violations. Furthermore, our experimental design allows for examination of particular factors and exposes the nuance surrounding the matter in greater detail than is possible simply by surveying preferred digital legacy outcomes. For example, our results suggest that the access of a given set of postmortem data by commercial entities is fundamentally different to identical access by close individuals, which is consistent with prior works exploring contextual integrity (Martin & Nissenbaum, 2016, 2017, 2019) and with findings by Nakagawa and Orita (2022) suggesting reluctance to engage in commercial uses of postmortem data, even for personal profit. While there is, at present, little commercialization of postmortem data, our findings are indicative of a rejection of corporate or governmental loosening of privacy practices after a person's death. We argue that, rather than distinguishing between what is kept and what is not, the problem should be framed around the appropriate transmission of data when such contextual factors are taken into account. Further to the examined independent variables, our qualitative analysis suggests that the motivation, defensibility and relatability of the access are also important factors, which parallels other research around conditional sharing of otherwise private information under particular mitigating circumstances, such as contributing health data for the purpose of combating the COVID-19 pandemic (Gordon et al., 2021; Watson et al., 2021).

We also sought to investigate the presence of a phenomenon in which some people feel and/or express an interest in their continued privacy after death, but fail to act, which has been termed the posthumous privacy paradox (Holt et al., 2021; Morse & Birnhack, 2020). Our results add to the limited evidence supporting the existence of such a phenomenon, with evaluations of the importance of postmortem privacy strongly opposed by evaluations of effort spent protecting that privacy. Our scenario-based experimental paradigm further shows a considerable proportion of respondents treating their postmortem data as private, yet participants widely reported that they did not use tools that are currently available for supporting that privacy or for planning their digital legacy. These results are consistent with existing PIM research that has indicated that users tend to struggle with long-term data management and organization of large personal archives (Boardman & Sasse, 2004; Whittaker & Hirschberg, 2001; Whittaker et al., 2010). As such, we suggest that broader PIM problems such as information overload and deferred evaluation may be contributing factors to the observed tendency not to engage with legacy planning behaviors. The possibility that the problem is at least partly of an organizational nature is further supported in our findings by the apparent ease with which participants reportedly made judgments of appropriateness and permission for postmortem access. Thus, it may be motivation and simplification that are required in order to promote this kind of decision-making. However, we acknowledge that making discrete individual assessments of appropriateness is somewhat distinct

from the task of approaching one's legacy as a whole, and consider it likely that users do also typically avoid the issue as an emotion-focused coping strategy, as has previously been suggested (Pfister, 2017). Where other approaches to encouraging privacy-focused behaviors often rely on nudges and other regular engagements with the user (e.g. Jackson & Wang, 2018), the topic of one's own death is rather more sensitive and one that we expect most users would prefer not to regularly be reminded of. However, our participants' own experiences with the deaths of others appear to have been instrumental in motivating them to take preparatory actions of a more traditional nature. As such, we suggest that users may periodically feel motivated to take actions around their own postmortem data if adequately supported to do so by the systems that they use to manage their personal data and information.

We organize our discussion around three core issues relating to the problem of appropriate postmortem data management: a need for improved clarity of the deceased's intent (as informed by the individuality and complexity of evaluations of postmortem data flows); a proposal for contextually responsive information retrieval (in order to support those with postmortem roles to act appropriately and according to the deceased's intent); and a need for supporting recognition of potential future data value and uses (in order to prevent the loss of valuable data or information and protect against future misuses).

5.2. The need for clarity of intent

Our qualitative findings outline the importance of providing a deceased person's loved ones with the information and clarity that they need in order to manage their death effectively. We found this to be the case for those who tended toward postmortem privacy as well as those who tended toward openness. Several participants noted that they had taken action with respect to their traditional estate but did not feel equipped to create a plan with respect to their digital estates. We argue that, given the individual variance in our participants' evaluations of suitable data access behaviors after death, seen in both studies, there is a need for a means to provide specific and granular instructions for those who may find themselves responsible for managing the future of a deceased person's digital assets and data.

Our findings place vital status as one of several other contextual factors that might affect appropriateness of a given data flow. Aligning our approach to privacy with Nissenbaum's *Contextual Integrity* (Nissenbaum, 2004), we do not feel that a dichotomy of Public versus Private is an appropriately nuanced way to consider postmortem access. We argue that broad questions around this subject such as "should we continue to honor personal data privacy after death" or "who by default should get a person's data when they die" are insufficient, and that a much more granular approach is required whereby one's status as living or dead is considered to be one variable of many that may impact the appropriateness of a given data flow. Within Contextual Integrity theory, entrenched social norms are an important modifier of such evaluations, and our results imply that norms are less clear with respect to postmortem data, with the possible exception of unauthorized access by companies or organizations. This aligns with an apparent lack of encultured practices identified in prior qualitative work (Pfister, 2017). With time, it may be that privacy norms emerge, given that people have been shown to align their privacy behaviors with others via imitation or reciprocity (Acquisti et al., 2015).

As it stands, users who are unsatisfied with an "all-or-nothing" approach to postmortem privacy are very unlikely to engage with digital planning or curation behaviors; to our knowledge, there is no existing infrastructure that is sufficiently capable of capturing the circumstances under which, or purposes for which, that data might be accessed. For example, it may be appropriate for someone to access their chosen means of communication in order to contact important people and inform them of their passing – an activity that is likely to be in the best interests of the deceased and their loved ones. However, the appropriateness of the access depends on the right person accessing the right information at the right time and for the right reason, and may be subject to restrictions – such as

not using the communication platform in a way that impersonates the deceased. This echoes prior work suggesting that some digital legacy technologies and activities may be considered valuable or appropriate only when used in the right context (Thomas & Briggs, 2014). This is therefore not just a problem of enabling access to data that had previously been private (which to some extent is already achievable, if complex, through legal or technological means) but also providing the new accessor with clarity and understanding about the information that is available to them and how it should be used – what has previously been labeled the “role inheritance problem” (Massimi & Baecker, 2010).

5.3. Contextual information management

Our qualitative findings illuminate how people typically expect a close relation to act as their representatives and are broadly willing to transfer decision-making responsibilities to them. However those representatives are expected to navigate increasingly large and complex personal datasets with little guidance with respect to suitable information-seeking behaviors or any particular actions that should or should not be taken. This finding is consistent with previous research showing the deferral of decision-making and consequential potential burden caused by postmortem data (Brubaker et al., 2014; Doyle & Brubaker, 2023; Gulotta et al., 2013; Odom et al., 2010; Pfister, 2017).

We propose that the traditional folder approach used in PIM, in which files and folders are placed in one location known to the user (Bergman & Whittaker, 2016), may limit appropriate discovery in a postmortem context. This is because the accessor, unfamiliar with the layout, may be required to look in many different locations whilst seeking some particular item. Such difficulties have been observed in prior research, in which users appear to be impeded by the different strategies used by others when attempting file retrieval in GIM environments (Bergman et al., 2014; Berlin et al., 1993). In the case of postmortem access, we suggest that retrieval may be impeded further still, as the deceased user may not have organized their files and data in a manner intended to be understandable to others. That the postmortem accessor might need to manually check much of the file system in order to find what is needed is not only time-consuming and emotionally burdensome, but may go against the wishes of the deceased (seeking privacy) and the accessor (seeking to be respectful). We also suggest that search functionality is not likely to be useful in a postmortem context, as the searcher will not be guaranteed to know the name or characteristics of what they seek. Instead, we argue that the organization of the information might be restructured according to the context of the access (in this case, after death and by a particular accessor). We suggest that in a more responsive informational environment, the accessor could be presented a sub-collection of information that is appropriate to their role and relationship and which is structured in a way that would be intuitive to them. In this way, a contextually sensitive information management system could build on sophisticated access control mechanisms such as Attribute-Based Access Control (ABAC), in which various attributes of users, resources and the system environment are used to dynamically determine access (Hu et al., 2015; Servos & Osborn, 2017). In the case of an assigned data steward, for example, postmortem access might reveal a concise and orderly set of folders and files containing relevant data that, for the deceased user, had appeared scattered across many folders amongst other information. Other loved ones might see a collection of photos, music and biographical information that could support them in their efforts to remember or memorialize the deceased. A system that achieved such aims would have satisfied the shared interests of all parties, in that the data subject’s wishes could be respected, the appropriate range of digital entities could be preserved and utilized, and the deceased’s loved ones could have clarity about the boundaries and responsibilities that they need to navigate.

Such a system, we argue, would partially conform to the user-subjective approach suggested by Bergman et al. (2003), in that information items related to the same subjective topic would be classified together and the importance of information would determine visual salience. However, it would differ with respect to the principle in which information should be retrieved and viewed in the

same context in which it was previously used. This deviation is logical, given that their reasoning for this principle was based on supporting the recall of the user who had placed the information there, which in a postmortem context is irrelevant. Doyle and Brubaker (2023) identify a challenge of this nature around mapping “pre-mortem data to post-mortem purposes.” We thus argue that digital legacy systems should be able to play the role of what Markus (2001) describes as a *knowledge intermediary* - one “who prepares knowledge for reuse by eliciting it, indexing it, summarizing it, sanitizing it, packaging it, and who performs various roles in dissemination and facilitation.” In doing so, the system could support the decontextualization and appropriate recontextualization of information (Ackerman & Halverson, 2004), in which superfluous or confusing contextual elements are stripped away and explanatory annotations or other supporting data are added in order to support comprehension by a “dissimilar other” (Lutters et al., 2007; Markus, 2001). Such a system would further cater to the individual differences and multiple strategies that have been exhibited by users of file management systems (Boardman & Sasse, 2004). We suggest that GIM systems are well positioned to integrate such contextually mediated information retrieval and we highlight PDS ecosystems in particular as an area of high potential for serving as a cross-service knowledge intermediary in this way.

However, our results also indicate the lack of effort exerted by users toward deliberative planning for death. Therefore, the question arises of how systems might be provided with the information required to carry out this role as intermediary. To this, firstly we suggest that legacy planning be considered an optional use case within a wider information management system. The ability to arrange for certain data access after death is arguably a small extension to arranging for data access under any other restriction or condition. Thus, one approach may be to support functionality that can group items or collections and assign user-defined properties and behaviors to them (e.g. via tagging), such as which other users have read/write privileges, how long the items should be retained for, or whether the visual salience of the items should be raised or lowered under certain conditions. We argue that such functionalities have many applications for user agency and negotiability beyond digital legacy purposes. A user may then also create, if so inclined (e.g. in a moment of motivation following a provocative event like a bereavement or diagnosis of illness), tags and annotations that determine and support postmortem access. This could be conducted in as much or as little detail as preferred, such as by simply expressing a default case for access permissions after death, and using the approaches that align with their individual information management strategies. Crucially, they would be able to do so without seeking and learning how to use a dedicated tool. An alternative approach to simplifying the task for the user may be to design an AI tool that is capable of organizing files and data based on written instructions. In this case, it may be possible to bring the process more in line with traditional will-writing, with an individual’s intent written in plain language. Unlike traditional wills, however, such a system would be able to offer the user a preview of their legacy as it would be experienced by others, and the opportunity to refine it further. In the case of either approach, we suggest that there is scope for the organizational burden of both digital legacy planning and postmortem data access to be decreased.

5.4. Illuminating latent value in mundane data

We believe that one of the main challenges to digital legacy planning is the identification of data that has latent value or hidden future uses. This difficulty was identified in work by Gulotta et al. (2013), which reported that participants found it difficult to see the value in their digital information for future generations. Likewise, Pfister (2017) reported a challenge of appraising and selecting data to be passed on. Our interview findings showed that predicted value is located in the expected places – things that historically have been handed down (photos, writing, stories), which is also consistent with earlier findings (Doyle & Brubaker, 2023; Gulotta et al., 2014). However, we also found that many participants, despite having never thought of it before, were excited (or in some cases,

dismayed) by the thought of more mundane data being used in the distant future to reconstruct their activities and support social history. Prior research has found that whilst passing on historical information can be seen to be important, acceptance is modulated somewhat by the intimacy of the personal information or its application (Thomas & Briggs, 2014), and Gulotta et al. (2014) identified an opportunity to integrate such information into broader cultural legacies. The unforeseen application of personal data is hypothetical; we cannot predict with any confidence that the ways that data will be used (or the value that people will place in the activities of their forebears) decades or centuries in the future will resemble what we are accustomed to. That there will be unforeseen uses of data of some kind, however, is difficult to argue with. In recent years we have already seen users of technology taken by surprise by the sudden value of seemingly mundane personal data, with data commonly referred to as the “new oil” and widely held to have disrupted large-scale power dynamics (Zuboff, 2015). At the time of writing, we are also experiencing major developments in the power and availability of artificial intelligence and machine learning. Even with what is available today, it is possible to produce realistic chat agents (Han et al., 2022), images and videos (Seow et al., 2022), and audio (Wang et al., 2023) that could be used to produce convincing representations of the dead, given only modest datasets. Voice recordings were identified by Massimi and Baecker (2010) to be of unexpected value to the bereaved but often created incidentally and not for remembrance purposes, and it may be that users of increasingly popular voice-activated technologies unknowingly produce datasets of high potential meaning but which are of ambiguous privacy status. It is also feasible that, with access to combined data from across a person’s life, data models could identify and reveal elements of their life that had never been intended to be public. Unfortunately, the ways that such technologies function are sufficiently complex that even advanced users are unlikely to recognize the ways that their data could be exploited. A similar conclusion was reached by Nakagawa and Orita (2022), who found that participants largely would not allow their personal data to be public and readable after death, but suggested that part of this reluctance may be due to their participants’ difficulty imagining specific users for their data after death.

We argue that, separate from the need to support postmortem privacy and handling of digital estates, there is a need for people to be able to better identify potential postmortem uses of their data and manage their data practices to support/prevent those uses as they see fit – including data that is observed, derived, or collated by organizations and which typically escapes the notice of most users. This we term as an HDI problem – supporting *legibility* and *agency* about data and its future uses, under circumstances under which the data subject or owner can no longer be expected to *negotiate* their boundaries. We propose that PIM is one research field that has the potential to support users to make sense of their data, what it says about them, and what it can be used for. To this end, we identify a need for future design development that supports 1) the identification by the user of potential combinations of their data and 2) their agency to impact, whether through legal, social, or technological means, the uses to which their future and postmortem data may acceptably be put.

5.5. Limitations and future work

The research presented in this paper is limited in some key ways. Our Study One quantitative findings used a sample ($N = 108$) that is too small to be considered generalizable to the population, nor suitably stratified to make this claim. The sample used for Study Two, while demonstrating a variety of ages, does skew toward older participants, which may lower their likelihood to engage with some behaviors associated with sensitive data and files, such as sexting (Galovan et al., 2018). Further, given the advertisement of the study as relating to death (in order to mitigate ethical risks), there is the possibility that our sample might be affected by selection bias. Also, the sample comprised of UK residents, and we would anticipate differences in results with populations from other countries and/or cultures. Our research aims were not to represent the beliefs of a wider population, but to demonstrate any differences within subjects according to context. We did not focus on religion, despite the large effect this might have on beliefs and thought processes with

respect to death and what happens after. We believe this is an important side of the research that should be tackled, but we decided in this case that religion should remain implied as a likely factor in individual differences and not explored experimentally due to likely difficulties being adequately representative. Similarly, we acknowledge that our choice of data types was limited, representing only a fraction of the variance and nuance that is truly present within one's personal information and data. Within the data types that we chose, there is also considerable room for making interpretations, assumptions, and for relational factors. Furthermore, some of those most likely to prefer complex digital legacy plans are those who are particularly prolific users of technology and personal informatics. We suggest that design work with such users is a suitable next step for the development of PIM systems with adequate postmortem functionality. We also acknowledge that there are ambiguities within the scenarios and wording used, and that interpretations of the term "appropriate" may differ. We feel that this ambiguity allowed us to gather responses that reflected natural responses to the scenarios without forcing participants to take a firm stance on the issue of posthumous harm. However, in addition to the suggested areas for design contributions identified in our discussion, future research expanding more directly on our findings might consider the development of more robust and validated measures, as well as a more varied and precise selection of data access flows.

6. Conclusion

In this paper, we have reported on the findings of novel mixed-methods research to examine the impact of context on appropriateness of postmortem data access and the associated difficulties for the formation of digital legacy plans. Our quantitative findings illustrate that the appropriateness of postmortem data flows is highly individual and differs significantly according to contextual factors such as the data type affected and who the accessor is. Reported effort spent protecting postmortem privacy interests is disproportionately low compared to the reported importance of those interests, and usage of existing processes and dedicated tools is uncommon. Our qualitative findings illustrate that whilst participants mainly identify file-based digital assets in their considerations for legacy plans, there may be latent value in mundane data that is evident only under particular contexts and perspectives. Participants spoke of shared interests between the living and the deceased in appropriate postmortem access, mutual responsibility in the communication of intent and sharing of data, and the expectation that postmortem data access and sharing is done in good faith and in accordance with those shared interests and responsibilities. We identify strategic design opportunities for information management systems to act as a knowledge intermediary between a deceased user and living users in order to promote appropriate and effective access whilst clarifying value and intent.

Acknowledgments

This work was funded through the EPSRC Centre for Doctoral Training in Digital Civics at Newcastle University (EP/L016176/1). We would like to thank all participants for contributing their time, and Voice for assisting with recruitment. We would also like to thank our anonymous reviewers for their time and valued feedback.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The work was supported by the EPSRC Centre for Doctoral Training in Digital Civics [EP/L016176/1].

Notes on contributors

Jack Holt is a PhD candidate at Open Lab, Newcastle University. His work explores issues of digital legacy and post-mortem privacy, and how technology can help support expression of personal data access and usage intent.

Jan David Smeddinck is an HCI researcher with expertise in interaction design, serious games, and machine learning, focused on digital health. He serves as Co-Director and Principal Investigator at the Ludwig Boltzmann Institute for Digital Health and Prevention.

James Nicholson is an Associate Professor at Northumbria University. His work focuses on human-centred cybersecurity, in particular how older members of the community can protect themselves from cyber attacks.

Vasilis Vlachokyriakos is a Reader (Associate Professor) of Human-Computer Interaction and Digital Civics at Newcastle University, UK and co-founder of Open Lab Athens. His work centres on designing and developing digital systems to support democratic practices and prevent harms and exclusions online. To undertake such research, Vasilis works in collaborative and interdisciplinary projects with local communities, third sector and public sector organisations by employing technology design-led, participatory and action research methodologies. Vasilis is currently an investigator on the EPSRC Centre for Digital Citizens and on the EPSRC Agency projects.

Abigail C. Durrant is Professor of Interaction Design at Newcastle University, UK. Abigail is Co-Director of Open Lab, an interdisciplinary research group in Human Computer Interaction (HCI). Practicing research through design using collaborative (co-)creative methods, she has a longstanding interest in understanding how interactions with emerging technologies shape our sense of selfhood, wellbeing, and our relationships with others.

References

- Ackerman, M. S., & Halverson, C. (2004). Organizational memory as objects, processes, and trajectories: An examination of organizational memory in use. *Computer Supported Cooperative Work (CSCW)*, 13(2), 155–189. <https://doi.org/10.1023/B:COSU.0000045805.77534.2a>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aal465>
- Albers, R., Sadeghian, S., Laschke, M., & Hassenzahl, M. (2023). Dying, death, and the afterlife in human-computer interaction. A scoping review. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–16. <https://doi.org/10.1145/3544548.3581199>
- Apple. (n.d.). *How to Add a Legacy Contact for Your Apple ID*. Retrieved February 17, 2023, from <https://support.apple.com/en-gb/HT212360>
- Bassett, D. J. (2022). *The creation and inheritance of digital afterlives: You only live twice*. Springer.
- Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research*, 40(3), 477–500. <https://doi.org/10.1086/671052>
- Bergman, O., Beyth-Marom, R., & Nachmias, R. (2003). The user-subjective approach to personal information management systems. *Journal of the American Society for Information Science and Technology*, 54(9), 872–878. <https://doi.org/10.1002/asi.10283>
- Bergman, O., Gutman, D., & Whittaker, S. (2022). It's too much for us to handle—the effect of smartphone use on long-term retrieval of family photos. *Personal and Ubiquitous Computing*, 27(2), 289–298. <https://doi.org/10.1007/s00779-022-01677-x>
- Bergman, O., & Whittaker, S. (2016). *The science of managing our digital stuff*. The MIT Press. <https://doi.org/10.7551/mitpress/9780262035170.001.0001>
- Bergman, O., Whittaker, S., & Falk, N. (2014). Shared files: The retrieval perspective. *Journal of the Association for Information Science and Technology*, 65(10), 1949–1963. <https://doi.org/10.1002/asi.23147>
- Berlin, L. M., Jeffries, R., O'Day, V. L., Paepcke, A., & Wharton, C. (1993). Where did you put it? Issues in the design and use of a group memory. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI*, 93, 23–30. <https://doi.org/10.1145/169059.169063>
- Birnhack, M., & Morse, T. (2022). Digital remains: Property or privacy? *International Journal of Law and Information Technology*, 30(3), 280–301. <https://doi.org/10.1093/ijlit/eaac019>
- BitWarden. (n.d.). *Emergency Access*. Retrieved March 3, 2023, from <https://bitwarden.com/help/emergency-access/>
- Boardman, R., & Sasse, M. A. (2004). “Stuff goes into the computer and doesn't come out”: A cross-tool study of personal information management. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 583–590. <https://doi.org/10.1145/985692.985766>
- Bowyer, A., Holt, J., Go Jefferies, J., Wilson, R., Kirk, D., & David Smeddinck, J. (2022). Human-GDPR interaction: Practical experiences of accessing personal data. *CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–19. <https://doi.org/10.1145/3491102.3501947>

- Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. SAGE.
- Brubaker, J. R., & Callison-Burch, V. (2016). Legacy contact: Designing and implementing post-mortem stewardship at Facebook. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2908–2919. <https://doi.org/10.1145/2858036.2858254>
- Brubaker, J. R., Dombrowski, L. S., Gilbert, A. M., Kusumakaulika, N., & Hayes, G. R. (2014). Stewarding a legacy: Responsibilities and relationships in the management of post-mortem data. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI*, 14, 4157–4166. <https://doi.org/10.1145/2556288.2557059>
- Brubaker, J. R., Hayes, G. R., & Dourish, P. (2013). Beyond the grave: Facebook as a site for the expansion of death and mourning. *The Information Society*, 29(3), 152–163. <https://doi.org/10.1080/01972243.2013.777300>
- Brucker-Kley, E., Keller, T., Kurtz, L., Parli, K., Pedron, C., Schweizer, M., & Studer, M. (2013). Passing and passing on in the digital world. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. <https://doi.org/10.1145/2998181.2998262>
- Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge analytica in major data breach. *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Chen, J. X., Vitale, F., & McGrenere, J. (2021). What happens after death? Using a design workbook to understand user expectations for preparing their data. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3411764.3445359>
- Crete-Nishihata, M., Baecker, R. M., Massimi, M., Campigotto, R., Kaufman, L. D., Brickman, A. M., Steinerman, J. R., & Black, S. E. (2012). Reconstructing the past: Personal memory technologies are not just personal and not just for memory. *Human-Computer Interaction*, 27(1–2), 92–123. <https://doi.org/10.1080/07370024.2012.656062>
- Dinneen, J. D., & Julien, C. (2020). The ubiquitous digital file: A review of file management research. *Journal of the Association for Information Science and Technology*, 71(1). <https://doi.org/10.1002/asi.24222>
- Doyle, D. T., & Brubaker, J. R. (2023). Digital Legacy: A Systematic Literature Review. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2), 1–26. <https://doi.org/10.1145/3610059>
- Edwards, L., & Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal*, 32(1). <https://doi.org/10.2139/ssrn.2267388>
- Elsden, C., & Kirk, D. S. (2014). A quantified past: Remembering with personal informatics. *Proceedings of the 2014 Companion Publication on Designing Interactive Systems - DIS Companion '14*, 45–48. <https://doi.org/10.1145/2598784.2602778>
- Elsden, C., Kirk, D. S., & Durrant, A. C. (2016). A quantified past: Toward design for remembering with personal informatics. *Human-Computer Interaction*, 31(6), 518–557. <https://doi.org/10.1080/07370024.2015.1093422>
- Epstein, D. A., Ping, A., Fogarty, J., & Munson, S. A. (2015). A lived informatics model of personal informatics. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp*, 15, 731–742. <https://doi.org/10.1145/2750858.2804250>
- European Commission. (2022). *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). *Official Journal of the European Union*, 119(1), 1–88.
- Facebook. (n.d.a). *What happens to my Facebook account if I pass away?* Retrieved February 17, 2023, from <https://www.facebook.com/help/103897939701143>
- Facebook. (n.d.b). *What is a legacy contact and what can they do with my Facebook account?* what is a legacy contact and what can they do with my Facebook account? Retrieved February 17, 2023, from https://www.facebook.com/help/1568013990080948?helpref=faq_content
- Fallatah, K. U., Barhamgi, M., & Perera, C. (2023). Personal Data Stores (PDS): A Review. *Sensors*, 23(3), 1477. <https://doi.org/10.3390/s23031477>
- Fiduciary Access to Digital Assets Act, Revised. (2015). <https://www.uniformlaws.org/viewdocument/final-act-with-comments-40?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments>
- Gach, K. Z., & Brubaker, J. R. (2021). Getting your Facebook affairs in order: User expectations in post-mortem profile management. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1–29. <https://doi.org/10.1145/3449248>
- Galovan, A. M., Drouin, M., & McDaniel, B. T. (2018). Sexting profiles in the United States and Canada: Implications for individual and relationship well-being. *Computers in Human Behavior*, 79, 19–29. <https://doi.org/10.1016/j.chb.2017.10.017>
- Gerdon, F., Nissenbaum, H., Bach, R. L., Kreuter, F., & Zins, S. (2021). Individual acceptance of using health data for private and public benefit: Changes during the COVID-19 pandemic. *Harvard Data Science Review*. <https://doi.org/10.1162/99608f92.edf2fc97>
- Gibbs, S. (2015, February 12). Facebook 'legacy contact' can take over your account when you die. *The Guardian*. <https://www.theguardian.com/technology/2015/feb/12/facebook-legacy-contact-can-take-over-your-account-when-you-die>

- Google. (n.d.). *About Inactive Account Manager*. About Inactive Account Manager. Retrieved February 17, 2023, from <https://support.google.com/accounts/answer/3036546?hl=en>
- Gouvernement de la République française. (2016). *La loi pour une République numérique*. <https://www.gouvernement.fr/action/pour-une-republique-numerique>
- Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). Edward Snowden: The whistleblower behind the NSA surveillance revelations. *The Guardian*. <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>
- Grimm, C., & Chiasson, S. (2014). Survey on the fate of digital footprints after death. *Proceedings 2014 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. <https://doi.org/10.14722/usec.2014.23049>
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, 18(1), 59–82. <https://doi.org/10.1177/1525822X05279903>
- Gulotta, R., Gerritsen, D. B., Kelliher, A., & Forlizzi, J. (2016). Engaging with death online: An analysis of systems that support legacy-making, bereavement, and remembrance. *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS '16*, 736–748. <https://doi.org/10.1145/2901790.2901802>
- Gulotta, R., Kelliher, A., & Forlizzi, J. (2017). Digital systems and the experience of legacy. *Proceedings of the 2017 Conference on Designing Interactive Systems*, 663–674. <https://doi.org/10.1145/3064663.3064731>
- Gulotta, R., Odom, W., Faste, H., & Forlizzi, J. (2014). Legacy in the age of the internet: Reflections on how interactive systems shape how we are remembered. *DIS '14: Proceedings of the 2014 Conference on Designing Interactive Systems*, 975–984. <https://doi.org/10.1145/2598510.2598579>
- Gulotta, R., Odom, W., Forlizzi, J., & Faste, H. (2013). Digital artifacts as legacy: Exploring the lifespan and value of digital data. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, 1813. <https://doi.org/10.1145/2470654.2466240>
- Gulotta, R., Sciuto, A., Kelliher, A., & Forlizzi, J. (2015). Curatorial agents: How systems shape our understanding of personal and familial digital information. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 3453–3462. <https://doi.org/10.1145/2702123.2702297>
- Han, S., Kim, B., Yoo, J. Y., Seo, S., Kim, S., Erdenee, E., & Chang, B. (2022). Meet your favorite character: Open-domain chatbot mimicking fictional characters with only a few utterances. *Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, 5114–5132. <https://doi.org/10.18653/v1/2022.naacl-main.377>
- Harbinja, E. (2022). *Digital death, digital assets and post-mortem privacy: Theory, technology and the Law*. Edinburgh University Press. <https://doi.org/10.1515/9781474485388>
- Harbinja, E., Edwards, L., & McVey, M. (2023). Governing ghostbots. *Computer Law & Security Review*, 48, 105791. <https://doi.org/10.1016/j.clsr.2023.105791>
- Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, 30(6), 377–386. <https://doi.org/10.1177/0270467610385893>
- 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>
- Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control. *Computer*, 48(2), 85–88. <https://doi.org/10.1109/MC.2015.33>
- Jackson, C. B., & Wang, Y. (2018). Addressing the privacy paradox through personalized privacy notifications. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2), 1–25. <https://doi.org/10.1145/3214271>
- Jones, W., Bruce, H., & Dumais, S. (2001). Keeping found things found on the web. *Proceedings of the Tenth International Conference on Information and Knowledge Management*, 119–126. <https://doi.org/10.1145/502585.502607>
- Kasket, E. (2012). Continuing bonds in the age of social networking: Facebook as a modern-day medium. *Bereavement Care*, 31(2), 62–69. <https://doi.org/10.1080/02682621.2012.710493>
- Kasket, E. (2019). *All the ghosts in the machine: The digital afterlife of your personal data*. Hachette UK.
- Kessler, J. (2019). Data protection in the wake of the GDPR: California's solution for protecting "The world's most valuable resource". *S Cal L Rev*, 93(1), 99.
- Khan, M. T., Hyun, M., Kanich, C., & Ur, B. (2018). Forgotten but not gone: Identifying the need for longitudinal data management in cloud storage. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–12. <https://doi.org/10.1145/3173574.3174117>
- LastPass. (n.d.). *Emergency Access*. Retrieved March 3, 2023, from <https://www.lastpass.com/features/emergency-access>
- Li, I., Dey, A., & Forlizzi, J. (2010). A stage-based model of personal informatics systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 557–566. <https://doi.org/10.1145/1753326.1753409>
- Locasto, M. E., Massimi, M., & DePasquale, P. J. (2011). Security and privacy considerations in digital death. *Proceedings of the 2011 Workshop on New Security Paradigms Workshop - NSPW, 11*, 1. <https://doi.org/10.1145/2073276.2073278>
- Lupton, D. (2016). *The quantified self*. John Wiley & Sons.

- Lush, A. (2014). Fundamental personal information management activities – organisation, finding and keeping: A literature review. *The Australian Library Journal*, 63(1), 45–51. <https://doi.org/10.1080/00049670.2013.875452>
- Lutters, W. G., Ackerman, M. S., & Zhou, X. (2007). Group information management. In: Jones, W., & Teevan, J (Eds.), *Personal information management* (pp. 236–248). Seattle: University of Washington Press.
- Maciel, C. (2013). *Digital legacy and interaction: Post-mortem issues*. Springer.
- Maciel, C., & Pereira, V. C. (2015). Post-mortem digital legacy: Possibilities in HCI. In M. Kurosu (Ed.), *Human-computer interaction: Users and contexts* (Vol. 9171, pp. 339–349). Springer International Publishing. https://doi.org/10.1007/978-3-319-21006-3_33
- Markus, L. M. (2001). Toward a theory of knowledge reuse: Types of knowledge reuse situations and factors in reuse success. *Journal of Management Information Systems*, 18(1), 57–93. <https://doi.org/10.1080/07421222.2001.11045671>
- Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Colum Sci & Tech L Rev*, 18, 176. <https://doi.org/10.2139/ssrn.2709584>
- Martin, K., & Nissenbaum, H. (2017). Privacy interests in public records: An empirical investigation. *Harv JL & Tech*, 31(1), 111.
- Martin, K., & Nissenbaum, H. (2019). What is it about location? *Berkeley Technology Law Journal*, 35(1). <https://doi.org/10.2139/ssrn.3360409>
- Massimi, M., & Baecker, R. M. (2010). A death in the family: Opportunities for designing technologies for the bereaved. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1821–1830. <https://doi.org/10.1145/1753326.1753600>
- Massimi, M., & Charise, A. (2009). Dying, death, and mortality: Towards thanatosensitivity in HCI *CHI'09 Extended Abstracts on Human Factors in Computing Systems*, 2459–2468. <https://doi.org/10.1145/1520340.1520349>
- Massimi, M., Odom, W., Banks, R., & Kirk, D. (2011). Matters of life and death: Locating the end of life in lifespan-oriented hci research. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11*, 987. <https://doi.org/10.1145/1978942.1979090>
- Meese, J., Nansen, B., Kohn, T., Arnold, M., & Gibbs, M. (2015). Posthumous personhood and the affordances of digital media. *Mortality*, 20(4), 408–420. <https://doi.org/10.1080/13576275.2015.1083724>
- Michels, J. D., Kamarinou, D., & Millard, C. (2019). Beyond the Clouds, Part 2: What Happens to the Files You Store in the Clouds When You Die? *Queen Mary School of Law Legal Studies Research Paper*, 316(2019), 31.
- Morse, T., & Birnhack, M. (2020). The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains. *New Media & Society*, 24(6), 1343–1362. <https://doi.org/10.1177/1461444820974955>
- Morse, T., & Birnhack, M. D. (2020). Digital Remains: The Users' Perspectives. In: Savin-Baden, M., & Mason-Robbie, V (Eds.), *Digital afterlife: death matters in a digital age* (pp. 107–126) CRC Press <https://doi.org/10.2139/ssrn.3397533>.
- Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). Human-data interaction: The human face of the data-driven society. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2508051>
- Nakagawa, H., & Orita, A. (2022). Using deceased people's personal data. *AI & SOCIETY*. <https://doi.org/10.1007/s00146-022-01549-1>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 41.
- Nissenbaum, H. (2009). *Privacy in context*. Stanford University Press.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Odom, W., Banks, R., Kirk, D., Harper, R., Lindley, S., & Sellen, A. (2012). Technology heirlooms?: Considerations for passing down and inheriting digital materials. *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems - CHI*, 12, 337. <https://doi.org/10.1145/2207676.2207723>
- Odom, W., Harper, R., Sellen, A., Kirk, D., & Banks, R. (2010). *Passing on & putting to rest: Understanding bereavement in the context of interactive technologies*.
- Ohman, C., & Floridi, L. (2018). An ethical framework for the digital afterlife industry. *Nature Human Behaviour*, 2(5), 318–320. <https://doi.org/10.1038/s41562-018-0335-2>
- Ohman, 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), 205395171984254. <https://doi.org/10.1177/2053951719842540>
- Pfister, J. (2017). 'This will cause a lot of work.': Coping with transferring files and passwords as part of a personal digital legacy. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW*, 17, 1123–1138. <https://doi.org/10.1145/2998181.2998262>
- Pitsillides, S. (2019). Digital legacy: Designing with things. *Death Studies*, 43(7), 426–434. <https://doi.org/10.1080/07481187.2018.1541939>
- Roberts, R. J. (2023). You're only mostly dead: Protecting your digital ghost from unauthorized resurrection. *Federal Communications Law Journal*, 75(2), 273–296.
- Seow, J. W., Lim, M. K., Phan, R. C. W., & Liu, J. K. (2022). A comprehensive overview of Deepfake: Generation, detection, datasets, and opportunities. *Neurocomputing*, 513, 351–371. <https://doi.org/10.1016/j.neucom.2022.09.135>

- Servos, D., & Osborn, S. L. (2017). Current research and open problems in attribute-based access control. *ACM Computing Surveys*, 49(4), 1–45. <https://doi.org/10.1145/3007204>
- STEP. (2022). *Don't Lose Your Memories Forever: STEP Calls on the Government and Service Providers Like Apple, Google and Meta to Do More to Help People to Pass on Their Digital Memories*. <https://www.step.org/press-office/dont-lose-your-memories-forever-step-calls-government-and-service-providers-apple-0>
- Stokes, P. (2015). Deletion as second death: The moral status of digital remains. *Ethics and Information Technology*, 17(4), 237–248. <https://doi.org/10.1007/s10676-015-9379-4>
- Thomas, L., & Briggs, P. (2014). An older adult perspective on digital legacy. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, 237–246. <https://doi.org/10.1145/2639189.2639485>
- Trevisan, D., Maciel, C., Pereira, V. C., & Pereira, R. (2023). Dead users' profiles on Facebook: Limited interaction beyond human existence. *Interacting with Computers*, 35(2), 262–275. iwad003. <https://doi.org/10.1093/iwc/iwad003>
- Uniform Law Conference of Canada (ULCC). (2016). *Uniform access to digital assets by fiduciaries act—progress report* (2015). <https://ulcc-chlc.ca/Civil-Section/Uniform-Acts/Uniform-Access-to-Digital-Assets-by-Fiduciaries-Ac/Uniform-Access-to-Digital-Assets-by-Fiduciaries-Ac>
- Vitale, F., Chen, J., Odom, W., & McGrenere, J. (2020). Data Dashboard: Exploring Centralization and Customization in Personal Data Curation. *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 311–326. <https://doi.org/10.1145/3357236.3395457>
- Vitale, F., Odom, W., & McGrenere, J. (2019). Keeping and Discarding Personal Data: Exploring a Design Space. *Proceedings of the 2019 on Designing Interactive Systems Conference*, 1463–1477. <https://doi.org/10.1145/3322276.3322300>
- Wallace, J., Thomas, J., Anderson, D., & Olivier, P. (2018). Mortality as framed by ongoingness in digital design. *Design Issues*, 34(1), 95–107. https://doi.org/10.1162/DESI_a_00479
- Walter, T. (2015). New mourners, old mourners: Online memorial culture as a chapter in the history of mourning. *New Review of Hypermedia and Multimedia*, 21(1–2), 10–24. <https://doi.org/10.1080/13614568.2014.983555>
- Wang, C., Chen, S., Wu, Y., Zhang, Z., Zhou, L., Liu, S., Chen, Z., Liu, Y., Wang, H., Li, J., He, L., Zhao, S., & Wei, F. (2023). *Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers* (arXiv:2301.02111). arXiv. <http://arxiv.org/abs/2301.02111>
- Watson, C., Ali, R., & Smeddinck, J. D. (2021). Tensions and mitigations: Understanding concerns and values around smartphone data collection for public health emergencies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–31. <https://doi.org/10.1145/3476071>
- Whittaker, S., Bergman, O., & Clough, P. (2010). Easy on that trigger dad: A study of long term family photo retrieval. *Personal and Ubiquitous Computing*, 14(1), 31–43. <https://doi.org/10.1007/s00779-009-0218-7>
- Whittaker, S., & Hirschberg, J. (2001). The character, value, and management of personal paper archives. *ACM Transactions on Computer-Human Interaction*, 8(2), 150–170. <https://doi.org/10.1145/376929.376932>
- Wobbrock, J. O., Findlater, L., Gergle, D., & Higgins, J. J. (2011). The aligned rank transform for nonparametric factorial analyses using only anova procedures. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 143–146. <https://doi.org/10.1145/1978942.1978963>
- Yamauchi, E., Maciel, C., Mendes, F., Ueda, G., & Pereira, V. (2021). Digital legacy management systems: Theoretical, Systemic and User's Perspective. *Proceedings of the 23rd International Conference on Enterprise Information Systems*, 41–53. <https://doi.org/10.5220/0010449800410053>
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>