Passing Down Passwords: How Older Adults Approach Postmortem Account Access and Digital Estate Planning

Jenny Tang
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
jennytang@cmu.edu

Xiaoyuan Wu
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
wxyowen@cmu.edu

Lujo Bauer
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
lbauer@cmu.edu

Nicolas Christin
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
nicolasc@cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
lorrie@cmu.edu

Abstract

Traditional estate planning practices enable people to provide their heirs access to the assets left behind but are often insufficient for the transfer and management of online accounts. To understand how estate planning practices could be improved, we conducted 21 semi-structured interviews with older adults in the United States that explored their practices, concerns, and needs regarding postmortem online account access and management. We encountered few formalized digital estate planning practices; many participants use their credential management practices—primarily pen-and-paper—to provide postmortem account access. How participants envision account transfer is motivated by trust in their current practices and in their heirs, while concerns regarding technology hinder adoption of new methods. Participants consistently prioritize accounts with financial assets, and expectations surrounding postmortem account management vary based on individual circumstances, with the common goal of reducing burdens on executors and heirs. Our results suggest the need for developing technical standardization and expert guidance for digital estate planning.

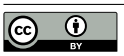
CCS Concepts

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**.

Keywords

Death, inheritance, password management, end-of-life, estate planning, digital legacy, older adults, aging, data management

ACM Reference Format:
Jenny Tang, Xiaoyuan Wu, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2026. Passing Down Passwords: How Older Adults Approach Postmortem Account Access and Digital Estate Planning. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3772318.3791633



This work is licensed under a Creative Commons Attribution 4.0 International License.
CHI '26, Barcelona, Spain
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3791633

1 Introduction

Closing out an estate and managing the affairs of a deceased individual is often a complex and difficult process for inheritors and executors, further complicated by the increasing importance of assets, digital or otherwise, that are accessed through online accounts. Without passwords or access to email accounts or phones for password reset, many heirs are left without the ability to log into those online accounts and access the assets, data, or memories they contain [30, 51]. As stories of loved ones being locked out of online accounts become more common, so too do articles and advice on how to conduct digital estate planning to reduce the burden on heirs [5, 25, 30, 43, 51]. Many of these articles advise adopting practices from traditional estate planning as well as using technical features and tools, and are often directed towards general audiences. Older adults are more likely to have engaged in estate planning than younger adults but may be less equipped to use technical tools that could help them more easily pass on their digital estates.

In this work, we examine older adults' approaches to digital estate planning. Digital estates encompass non-digital assets that are accessible via online accounts, such as money or utilities, as well as purely digital assets, i.e., "any object that has monetary and/or sentimental value and exists only in electronic form," such as cryptocurrency wallets or photos [40].

Most existing research on the management and transfer of online accounts after the death of the account holder explores *digital legacy* (rather than the digital *estate*), examining specific digital platforms, management or deletion of certain data, or expectations for the use of data. Work in digital legacy tends to focus on digital data and its sentimental and archival value [7, 9–11, 21, 47], or on how existing or proposed tools can properly enable others to manage those data after the passing of their owner [26, 32, 52]. However, digital legacy research usually does not focus on bank accounts or digital accounts that provide access to non-digital services.

We believe this is a critical gap in the literature. Indeed, the various accounts in a digital estate serve vastly different purposes: some accounts may be tied to significant financial assets, some may be needed for authentication processes to provide access to other resources, others contain irreplaceable memories, while still others may have been abandoned by the account holder and no longer have value. As a result, approaches to handling these accounts vary greatly depending on the accounts or data at stake [26, 52]. Some people may want to allow heirs to *take actions* on or manage

accounts (e.g., transferring or closing out financial accounts or payments), while others may want to simply provide access to account *contents* (e.g., photos, emails).

We investigate digital estate planning with a specific focus on how older populations provide heirs and executors access to their digital estates. Unlike most prior work, we focus on older adults, who are more likely to have already prepared estate plans and made arrangements for transfer of assets, digital or otherwise [57]. Scoping digital estate planning for older adults allows us to identify specific needs and challenges this population faces, placing value on more than the data contained in digital estates to understand how digital estate planning can complement traditional estate planning. We investigate existing practices for digital estates and where they may fall short and fail to achieve desired outcomes.

We conducted 21 semi-structured interviews with adults age 60 or older in which we discussed their digital estates and digital-estate-planning processes. Specifically, we explored the following three research questions:

- **RQ1** What steps do older adults take so that heirs will have access to their digital estates and what considerations underlie these practices?
- **RQ2** What barriers are older adults encountering during digital estate planning?
- **RQ3** What do older adults believe would be helpful in facilitating digital estate planning?

Participants were motivated to conduct digital estate planning to reduce the burden on their heirs and so that heirs had access to assets with monetary and sentimental value. Although digital estates were rarely formally discussed in estate planning, most participants reported using *ad-hoc* practices to grant account access to heirs, typically by directly sharing their passwords as an extension of their everyday password-management practices (§4.3). Most participants also assumed that their heirs would be able to infer what accounts are important, even without providing explicit instructions. All participants consistently viewed accounts with financial assets as the most important to pass on, and had varying preferences for other accounts, with most participants being less concerned about passing on digital data stored in their accounts (§4.2). Participants also mentioned a variety of barriers to managing passwords and planning for postmortem account access, sometimes exacerbated by struggles with technology (§4.4). Importantly, unlike younger populations who may find estate planning daunting and/or hold fewer financial assets but more digital data [26], older adults evaluated their digital estates within the context of their own existing estate planning, focusing more on accounts related to financial assets and less on those with data as ones they cared about passing down to heirs.

We propose approaches—and call for additional research—to make digital estate planning easier for older adults and lessen the burden on executors and heirs, drawing on parallels between digital and traditional estate planning and on the tensions between needs and current practices that emerged in our study (§5).

2 Related Work

As people increasingly use the Internet to access accounts and store personal documents, photos, and communications, it is becoming necessary to extend (or modify) traditional estate management practices for the digital realm. Here we review prior work on digital legacy that explores how people make decisions about what happens to digital accounts and data after death. We also review prior work on password sharing, a practice that may help facilitate digital estate planning. Finally, we review prior work that explores older adults' perspectives on digital legacy and online account management.

2.1 Digital Legacy and Digital Death

Digital legacy, at a high level, revolves around "the movement of data between the dead and the living, and the passing down of data between the living" [10]. As people increasingly store important information and assets digitally, new challenges to estate planning for such data and assets have appeared [27], and research on the topic has followed suit.

Much of the literature examines data management, what happens to data after the death of the owner, and account owners' wishes regarding how data is handled [7, 9, 21, 35, 47]. Data management research tends to primarily involve decisions about persistence or deletion of data [7, 11, 19, 32, 34, 45]. More recent work has examined planning for specific digital assets, such as cryptocurrencies [13]. The sheer number and complexity of accounts and associated data often present challenges for those engaged in digital legacy planning [11, 52]. Even though digital legacy encompasses a variety of accounts and account types, related work so far has primarily examined the management of data. However, some accounts (such as online banking) do not contain data that is generally considered part of digital legacy and are often not examined in detail in discussions of digital legacy, despite containing assets that are part of a digital estate. We aim to fill this gap.

Beyond the first steps of inventorying accounts, other difficulties arise in planning for what happens to data after death of the account owner. These include privacy and security concerns, such as with misuse of data or loss of control over identity representation, or simply general discomfort with others accessing one's data after death [12, 20, 26, 56]. In particular, questions about the existence or relevance of privacy rights for deceased individuals often arise [12, 23, 26]. Thus, due to the importance placed on data, privacy is often one of the main considerations in digital legacy work.

Some platforms already have methods to designate someone to manage the contents of an account after the owner's death [16]. Even so, technical barriers also exist, with designees encountering difficulties with using digital legacy features [17]. Technical tools and features may be misaligned with what users want or expect them to do, and may not be available for all types of accounts [17, 47]. Emotional and relational considerations also play a role: the designation of different stewards or people to receive the data or manage a digital legacy can be a difficult and emotionally fraught decision [11, 52]. Even though older adults who have engaged in end-of-life estate planning may be emotionally comfortable thinking about what should happen to their digital traces after their death, technical barriers may make it challenging for them to implement their plans [56]. Though we are interested in technical tools and features, we also investigate current practices—whether technical or not—that people use to manage their digital estates,

including access to data contained in an account as well as the ability to manage or take actions on the account itself.

Legal issues, such as terms of use that prohibit allowing others to use one's account credentials or transfer accounts, may also pose barriers for planning for postmortem account management [1, 23, 32, 42]. Legal ambiguities erect further barriers for both those planning for digital legacy, as well as those working in the field, such as estate planners [41]. In fact, from a survey of estate practitioners, 39% would advise clients to share passwords as a means to ensure access, while 35% did not feel that password sharing was appropriate, often citing legal concerns [40]. Similarly, press articles also hint at murky legality: One *New York Times* article assumes that heirs had login information, but also notes that allowing non-account holders to access accounts may violate terms of service or be otherwise illegal [51]. Meanwhile, another *New York Times* article points to the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)—which gives executors legal authority to obtain access for managing digital assets postmortem—as the impetus for conducting digital estate planning [5, 22, 58].

Doyle and Brubaker conducted co-design sessions to understand what types of approaches are effective in planning for end-of-life data management [11]. They found that participants felt inventorying all accounts extremely difficult and burdensome, and that planning approaches that focused on relational values and closely facilitated by those running the workshop were much more helpful [11]. Indeed, trust and nature of personal relationships with the deceased also often arise as major factors impacting how data should be handled [7, 16, 17].

This line of work often examines preservation and data. In our work, we broaden the scope beyond data and legacy, to the digital estate: we examine the management of credentials as well as access to accounts and their associated assets rather than just access to account contents.

2.2 Password Sharing

Password sharing—whether through password managers, pen-and-paper, or other means—is an important way of ensuring others have access to online accounts, both before and after death. Passwords are shared for both convenience and necessity, and sharing is particularly common for everyday devices and accounts used by multiple people in a household [36, 49, 54, 55]. How people share accounts varies depending on how close those sharing the account are, and can evolve and change as that relationship changes [31, 46, 49].

While common, password sharing raises security concerns, particularly around password reuse [44]. Password managers are also often recommended as secure options, but non-expert users may not use them effectively [8, 50], be unfamiliar with them, or be uncertain of their security and trustworthiness [3, 8, 28]. Ray et al. found that older adults were particularly distrustful of security (and particularly cloud storage) for password managers, but advocates such as family members can help encourage adoption [53].

Account management and credential sharing methods for digital legacy include using cloud computing, password managers, or electronic data safes [26, 32, 52]. However, shared or joint accounts may present unique challenges for digital legacy, and the assumption that each account is only used by a unique user poses problems for shared accounts [1, 55]. Considerations for password sharing or password management also differ between young and older adults, with older adults more interested in sharing passwords for emergency, rather than ordinary, situations [53, 59]. However, password sharing remains a common practice, and we investigate it in the specific circumstance of postmortem online account management rather than for simultaneous account access.

2.3 Older Adults

Management of online accounts and assets for older adults may pose unique challenges, such as due to cognitive decline or changes in ability [15, 37]. Older adults sometimes have different perspectives and preferences for online accounts and account management than younger adults, and can face challenges due to perceived lower technical knowledge [15, 59, 60]. This suggests that older adults may face specific security, privacy, and password management concerns that can benefit from more tailored interventions.

Our work investigates the considerations, practices, and challenges of older adults in sharing credentials to allow their heirs access to digital estates after death. Prior work on digital legacy often recruited participants already familiar with digital legacy systems, who have technical training, or who are younger [11, 26, 52]. While some works have aimed to capture perspectives across age groups, including of older adults, they focus on expectations and values regarding data and digital representation after death [9, 56]. To our knowledge, we are the first to investigate the specific needs of older adults in digital estate planning, who—compared to younger populations—may have more financial assets that they have considered as part of their estate planning, while having fewer digital traces and thus place less value on data and digital legacy.

3 Methods

In this section, we discuss our recruitment methods, sample, study materials, as well as our coding process.

3.1 Recruitment and Sample

We recruited participants aged 60 years old and over, fluent in English, located in the U.S., and who had at least one online account. We chose 60 years as the lower age bound (there was no upper bound) as we expected participants in this group to have both considered their *own* assets and estates (whether digital or not), and to have had experience dealing with estates of others, e.g., their parents. However, having conducted estate planning was *not* a requirement to participate in the study.

We recruited through snowball sampling via email, starting with potential participants and those within the authors' networks who could refer potential participants. We complemented our snowball sample by putting up posters in various locations in a mid-sized city in the United States (Pittsburgh, PA) as well as on social media and mailing lists for older adults. Potential participants filled out an online survey that collected basic demographic information, total net worth, whether they had a will, and information about their online accounts. The survey concluded by asking respondents to enter an email address at which they would like to be contacted if they were interested in participating in an interview. The full text of the survey can be found in Appendix A. We received 63 responses

Table 1: Participant demographics for the interest survey and interviews.

	Interest Survey		Interview	
	Num.	%	Num.	%
Gender				
Female	30	54.55	11	52.38
Male	25	45.45	10	47.62
Age				
60 – 69	32	58.18	8	38.10
70 – 79	11	20.00	4	19.05
80 – 89	11	20.00	8	38.10
90 – 99	1	1.82	1	4.76
Race				
White	37	67.27	18	85.71
Black or African-American	17	30.91	3	14.29
Asian	1	1.82	0	–
Net Worth				
Less than $100K	2	3.64	0	–
$100K – $1M	12	21.82	7	33.33
$1M – $5M	23	41.82	10	47.62
$5M – $30M	7	12.73	1	4.76
$30M or more	9	16.36	2	9.52
Prefer not to say	2	3.64	1	4.76

to our interest survey. We excluded eight responses with duplicate email addresses, leaving 55 valid responses. We emailed interview invitations to 32 respondents, stratified for diversity in gender, age, race, and net worth. We conducted 21 total interviews. We provide demographic details of participants in Table 1.

As our study targeted older adults and addressed topics involving financial accounts, some potential participants were concerned our recruiting message might be a scam, and a few reached out directly to the project supervisors to confirm the study was legitimate. In subsequent recruitment rounds, we modified the recruitment material to provide the institutional email addresses of the project supervisors and encouraged potential participants to reach out for confirmation.

3.2 Interviews

We conducted 21 semi-structured interviews between March and September 2025, all over Zoom. The interviews ranged between 59 and 105 minutes long, and took 82 minutes on average. Prior to recruitment, we conducted four pilot interviews and used participant responses and feedback to iterate on and improve our interview script. The script can be found in Appendix B.

All interviews except one (conducted by a single author) were conducted with one author as the primary interviewer and another author taking notes and asking additional questions when relevant.

The first part of the interview asked about participants' general experience with estate planning, wills, and online accounts. This included understanding what plans participants have for management of their online accounts (e.g., email, online banking, social media, etc.), the specific online accounts they are most concerned about providing postmortem access to, and their current approaches to postmortem account access.

The second part of the interview asked participants' opinions about three potential means of providing inheritors with access to online accounts or their contents after death or incapacitation:

(1) **Account Sharing.** Some people provide account access to inheritors by sharing their password with them. Others set up family or joint accounts in which each partner or family member uses a separate username and password to access the account. We asked participants about their account sharing practices and their opinions on such methods in the context of postmortem account access.
(2) **Legacy Features.** Some platforms provide built-in legacy features—such as Google's Inactive Account Manager, Apple's Legacy Contact feature, or Facebook's Memorialization feature—that grant inheritors the ability to manage inactive online accounts or receive the data within [4, 18, 39]. We introduced legacy features to participants before asking whether they had used or would use these methods for postmortem account access, and their experiences or opinions on doing so.
(3) **Password Managers.** Password managers can generate, store, and automatically fill in passwords. Some password managers are built into browsers and operating systems, while others are third-party software. We gave a brief explanation of password managers and asked participants for their feelings regarding using password managers specifically as a means of postmortem account access.

For each of the above, we followed up with questions about what potential advantages or barriers participants think might arise in using each method for managing postmortem online account sharing. We drew the broad categories of barriers (technical, legal, emotional, security, and privacy) from prior work that investigated digital legacy (See §2.1).

We concluded each interview with a debrief to address any questions and provide information and links to any tools that participants wanted more information on. Participants were compensated with a $30 gift card.

Following an accepted practice in our field (for example, in [24, 29]), instead of identifying participants with numbers (e.g., P1), we use pseudonyms "to protect participants' identities and maintain confidentiality, while at the same time emphasizing that study participants are individuals, with unique voices and experiences, with whom readers can connect on a personal level" [33]. The pseudonyms we used were drawn from a list of the most popular male and female names in the United States in the 1940s. We sorted these names alphabetically by gender and assigned them to participants according to their gender identity [2].

3.3 Analysis

Following methods and guidance from prior work, two authors conducted a thematic analysis of the interview transcripts [6, 38, 48]. First, one author developed an initial codebook through inductive coding of a single interview. Using this preliminary codebook, both authors coded a second interview together to build familiarity with the codes and to expand the codebook as new themes emerged.

Next, the two authors independently coded three additional interviews using the updated codebook, adding new codes when additional themes appeared. They subsequently met to review all codes and resolved disagreements through discussion, either by merging semantically similar codes or incorporating newly identified ones. Using the reconciled codebook, the authors reached agreement (Cohen's $\kappa = 0.75$) on the three independently coded interviews. The final codebook (see Appendix C) was then applied to the remaining sixteen interviews, with one author coding five transcripts and the other coding eleven. All thematic analysis were performed using MAXQDA.[1]

3.4 Ethical Considerations

Our study was approved by our institutional review board (IRB). At the beginning of the interest survey, we presented participants with a consent form in which we introduced the full study procedure, risks and benefits, compensation, as well as how we store and protect participant data. Participants could only proceed to the interest survey after consenting. We began the interviews by obtaining participants' consent, including having their voice and video (for those who turned on their webcam) recorded. Participants were free to terminate the interview at any time. All interviews were recorded via Zoom and stored in our password-protected institutional Zoom accounts. As described in Section 3.2, we replaced all participant names with pseudonyms before data analysis.

4 Results

We found that participants' approaches to digital estate planning were generally *ad-hoc* and informal, but followed similar considerations as in traditional estate planning. In this section, we start with a brief overview of participant demographics (§4.1). We then organize our results around the themes derived from our interviews, specifically motivations, priorities, and expectations for digital estate planning (§4.2); continuation of premortem practices for postmortem management (§4.3); preference for familiar non-technical approaches (§4.4); and desire for features, tools, and guidance to make digital estate planning easier (§4.5).

4.1 Participant Demographics

We interviewed 21 people: eleven female and ten male participants between 60 and 91 years of age. Participants' self-reported net worth ranged from US $100K to over US $30 million. Detailed demographics of participants for both the interest survey and the interview are in Table 1. Pseudonyms of interview participants with demographics can be found in Table 2.

In the interviews, all participants stated they have financial (e.g., banking, investment) and email accounts, almost all participants have social media, and most participants pay bills (e.g., utilities, phone) online and have travel-rewards accounts and online-storage accounts. Table 3 in Appendix C provides a detailed breakdown per account type.[2]

[1]https://www.maxqda.com/

[2]The self-reported account ownership information from the screening survey sometimes contradicts interview responses, e.g., two participants did not select "email" in the survey, despite all participants having email accounts through which they scheduled interviews.

Table 2: Interview participants' pseudonyms and demographics.

Name	Age	Gender	Race	Net Worth (USD)
Alice	80	Female	White	$1M – $5M
Arthur	67	Male	White	$100K – $1M
Barbara	65	Female	White	$1M – $5M
Bruce	78	Male	White	$1M – $5M
Carol	82	Female	White	$1M – $5M
Charles	77	Male	White	$1M – $5M
David	85	Male	White	$1M – $5M
Donna	84	Female	White	$30M or more
Edward	80	Male	White	$1M – $5M
Elizabeth	79	Female	White	$1M – $5M
Frances	80	Female	White	$100K – $1M
Frank	68	Male	White	$100K – $1M
Gary	65	Male	Black	$1M – $5M
Gloria	83	Female	White	$1M – $5M
Harold	62	Male	Black	$100K – $1M
Helen	84	Female	White	$100K – $1M
Irene	67	Female	White	$100K – $1M
Karen	61	Female	Black	$30M or more
Larry	91	Male	White	Prefer not to say
Linda	70	Female	White	$100K – $1M
Michael	60	Male	White	$5M – $30M

4.2 Motivations, Priorities, and Expectations for Digital Estate Planning

We found that participants' motivations, priorities, and expectations for digital estate planning were often similar to those they had for traditional estate planning. Specifically, the main motivations underpinning digital estate planning were providing access to important assets—data or otherwise—and easing the burden on heirs. The financial or sentimental value of accounts in the digital estate influenced the prioritization of which accounts to pass on, similar to considerations in traditional estate planning, which focuses primarily on financial assets or valuable goods.

However, participants generally expected that providing account credentials would be sufficient to pass on online accounts to heirs—similar to designating inheritors in traditional estate planning—and did not consider other intricacies of access relevant to digital estates, such as two-factor authentication (2FA). Participants also expected heirs to intuitively understand which accounts were relevant to handle postmortem, even without explicit instruction.

4.2.1 Account prioritization. Though the interviewer asked participants about all accounts they reported in the interest survey, all participants tended to focus on accounts with financial assets and consistently identified financial accounts as the most important for postmortem sharing. One participant, Bruce, said "Outside of my financial accounts. I really don't care." Participants rarely distinguished between providing access to manage accounts (for example, to close them) and providing access to the contents of the account. In most cases, participants' views on postmortem sharing

of non-financial accounts varied based on the monetary value, sentimental value, and practical value and initially primarily focused on the data in accounts.

Financial accounts are most important. All participants said they already had or were in the process of including accounts that contain monetary assets (e.g., banking, stocks, pensions, etc.) in their wills and estates. About half of participants expressed trust that the legal process of closing out an estate would allow their beneficiaries to access the contents of their financial accounts through the institutions (such as banks) that manage these accounts. However, some participants raised concerns that the bureaucratic process would take a long time, and wanted their heirs to be able to access these accounts immediately if necessary, for example to cover medical or funeral costs. In such cases, providing login information was seen as a benefit for the timely management of and access to the contents of such accounts.

Unlike traditional financial assets, cryptocurrencies are purely digital assets, tied to credentials rather than the identity of the account holder, with no alternative access methods to the stored value. Three participants had cryptocurrency holdings, and none had planned for postmortem transfer of those assets, which is in line with prior work finding that most cryptocurrency users had not planned for transfer of wallets after death [13]. These participants were unconcerned because they did not have what they deemed to be significant monetary assets in cryptocurrency accounts.

Some accounts need timely management. In addition to accounts with access to financial assets, participants also mentioned the need for timely management of accounts with their credit cards linked, such as shopping accounts, and accounts that have automatic withdrawals, such as auto-paid utility bills or entertainment subscriptions. Most participants had initially only considered the data contained in these accounts (e.g., bill history, order history)—which would not be considered relevant for traditional estate planning—and dismissed them as unimportant. No participants felt that entertainment accounts were important to pass to heirs, but a few mentioned that it was important to stop the recurring payments. Thus, the importance was not based on the contents of these accounts, but rather on the management of these accounts and their timely closure to prevent further charges or misuse of the linked credit cards by unauthorized users. These financial considerations raised new questions that some participants did not consider before the interview and prompted participants to realize the importance of timely management of online accounts with potential financial implications.

Importance of rewards accounts depends on their holdings. Most participants owned travel-rewards accounts, where reward points can be redeemed for goods and services. Participants' evaluations of the importance of such accounts varied depending on their holdings. For example, Barbara expressed wanting her heirs to be able to use her points to book travel. In contrast, some participants were less concerned about postmortem sharing of travel-rewards accounts due to there being few accumulated points in those accounts. In some cases, participants were unsure whether points could be transferred. In such cases, it was seen as useful to provide account credentials for heirs to access and use the points rather than determining a method of transferring these points.

Accounts with practical value are often overlooked. Credentials to emails, phones, and device accounts that could help heirs pass two-factor authentication (2FA) hold practical value during the digital estate management process, but some participants initially overlooked them due to focusing on the data (or absence thereof) in those accounts and the lack of tangible assets *directly* controlled by those accounts. For example, email accounts can be used to receive important notices, provide two-factor authentication, or even as a recovery mechanism to gain access to other accounts. When reflecting beyond content in these accounts, participants noted the importance of emails as a *keystone account* for digital estate management. While one participant noted that important documents were stored in their email accounts, and therefore wanted their heirs to have access to their email, most other participants did not find the contents of email important to pass on, but rather wanted to provide access to email accounts for the purpose of allowing the management of other accounts tied to those email addresses. Indeed, even though Irene noted that "The last ones [to close] would have to be email because they're gonna need access to my email to get everything else closed out," she also remarked, "There's no need to even share the content with anybody, because it's gonna be meaningless to my siblings."

During interviews, about half of participants reflected upon the complex ways in which different accounts and verification methods interacted with and depended upon each other. In particular, while almost all participants had accounts that used 2FA, many had not explicitly thought about 2FA when planning on transferring account access. The 2FA devices mentioned were either phone or email, and most participants were confident that heirs could access these authentication methods.

2FA was necessary for accounts that participants deemed important—such as banking accounts—prompting participants to raise concerns about 2FA preventing their heirs from accessing these accounts. David, for example, noted that phone bills would have to be removed last so that 2FA would continue working until that point and that explicit instructions may be needed so that heirs are aware of the dependencies.

> I'll make [a] note in my little listings of things. Should verification be required...[it]...will come on my cell phone, so...don't close out the cell phones for a while.
> *–David*

When reflecting on 2FA, participants brought up other credentials, such as phone passcodes or laptop passwords as important for heirs to be able to manage their online accounts. Some also noted that the credentials to access physical devices (such as phone or laptop passcodes) were already in their records of credentials, while others realized that they needed to explicitly provide this information. Even though some participants used biometrics (such as Face ID) to access certain accounts on their devices, they were confident heirs would be able to obtain access through fallbacks, such as using phone passcodes.

Medical and health-related accounts were also seen to hold practical value. Health and insurance portals allow heirs to pay medical bills and access family medical history. Participants wanted heirs to

have access so medical bills can be paid. One participant explicitly stated wanting their family to know about their health history by accessing such accounts.

Varying opinions on how to handle accounts that carry sentimental value. Some participants mentioned that accounts (e.g., social media, online photo storage) could have sentimental value for heirs. However, most participants stated providing their heirs access to social media accounts was not important as they rarely posted on those platforms. Even so, some discussed social media account deletion, memorialization, and legacy features, mostly in the context of how they felt seeing social media posts about their deceased friends' birthdays.

> It's there, and every time her birthday comes around, people are posting on her page, and ... I know they all know she's deceased. But so yeah, kind of macabre at that point. *–Irene*

After discussing these notifications and persistence of social media accounts of deceased friends, some participants expressed more interest in having heirs manage these accounts, though most remained unconcerned about passing on the contents of those accounts.

Most participants used online storage, but were divided on the importance of passing on such accounts. Some participants stated their heirs already had access to photos in the cloud, or that they sent photos to their families on a regular basis. These participants did not feel the need to provide postmortem access to heirs for online storage accounts, as the most important memories were already shared.

> They have the pictures and things that I've shared with them. ... [for pictures on iPad], they can just look and then delete. *–Linda*

Privacy did not come up as a reason for not providing access to online storage accounts. Instead, the reasons include personal preference, beliefs that the data would not be of interest to heirs, or a desire to reduce the burden and information heirs would have to sort through.

Other participants wanted to share the stored memories, and about half of the participants wanted to have granular control over what is shared in these accounts, passing down photos of family and fond memories, without sharing mundane content such as Helen's "close to a thousand screenshots that I...need to go in and clean out."

4.2.2 Assumptions about postmortem account management. About half of participants did not create formal instructions for some or all accounts, but assumed that heirs would figure it out, understand their wishes, or intuitively know which accounts were important to handle. Most participants stated that they had not thought much about how heirs would handle their digital estates prior to the interview. For example, Frank said "That's up to my nephew, I guess". Similarly, Edward notes the lack of instruction for his digital estate.

> I assumed they would sit down with my list of accounts ... and say, ...Don't know why he had this one, get rid of it... But it's not a formal thing, it's not something in my will, it's not an agreement. *–Edward*

Participants also considered the personal traits of the executors. For Irene, knowing that her family members are tech-savvy provided some comfort that her accounts would be properly handled. However, Frances noted that her family members are disorganized and reflected on the need to provide more explicit instructions on how to handle accounts. Beyond executors and heirs, some participants were confident that their executor would be able to rely on their attorney, banker, or other professional for assistance either for management of the accounts or access to their contents as they would with traditional estate planning.

While a few participants had general concerns about privacy of their online accounts with respect to the general public, no participants had concerns related to allowing heirs and executors to access their accounts after their passing, stating they have nothing to hide from their family.

> After I'm dead, then there should be no limitations to how much they're able to have access. *–Gary*

4.2.3 Easing the burden on executors and inheritors underpins motivation for digital estate planning. Steps that participants had taken or were thinking of taking to make it easier for their executors to manage their digital estate included: providing explicit instructions, having discussions about their wishes and expectations, slowly migrating and transferring control over accounts prior to death, reducing the number of active accounts, and using automatic account-closure features to minimize the number of accounts that need to be manually handled.

A few participants shared stories from people they know who faced difficulty accessing online accounts after the abrupt passing of loved ones. Negative experiences motivated some participants to reflect on the burden their own digital estate might impose on others, while positive experiences with traditional estate management similarly encouraged them to ensure that their heirs would receive the same ease and clarity they themselves had benefited from.

> She had everything lined up, and it was so simple for my daughter, my sister, and I to close out her estate. ... it was just so easy ... everything's taken care of... Considering what I have seen people go through with their loved ones, and then contrasting it to the situation with my mother, I thought, we're gonna get this as organized as we can. *–Frances*

Some participants said they did not want to burden their heirs with accounts containing large volumes of data that might be time consuming or overwhelming to sort through. This led participants to state that they did not care what happened with those accounts or to choose not to share some accounts.

> I don't want to have a burden on the kids that they feel that they have a problem. If I destroy this picture or something, you know, Mom or Dad would have a problem with that. ... I don't want to have them to have to go through that decision process. *–David*

Some participants also reflected that even if some accounts were missed, as long as the important (financial) accounts are properly passed on, all would be well. This follows similar trends as in traditional estate planning, prioritizing providing heirs with access to financial assets. The focus on accounts with financial value may

also partially stem from a desire to minimize the number of accounts the bereaved would have to manage, minimizing burden. A few participants took a lighthearted approach, stating that they would be dead, so what happens to those accounts would no longer really matter to them personally.

> It's very tempting to try to manage things after you're gone, but I don't think I believe in that. I think whenever I'm incapacitated or die, I'm sure they'll do just fine, and whatever they want to do is fine with me. –*Gloria*

4.3 Extending Current Credential Management Practices for Postmortem Account Sharing

Participants' current practices related to planning for postmortem account access were generally *ad-hoc* and informal, and were based on the credential management practices that participants were already using, trusted, and found convenient. From here on, we will mostly equate credentials to "passwords," since passwords were the most frequently mentioned type of credential, but the findings may be extended to other credentials that can be passed down in a similar manner as passwords (e.g., passcodes for phones). No participants mentioned using passkeys or physical tokens for authentication. Most participants reported that they have already shared their account credentials with the inheritors they trust, both to facilitate postmortem access and to allow for ongoing assistance with account-management tasks. Despite participants' general confidence in their existing practices for managing their digital estate, tensions between the desired outcomes and existing practices remain.

4.3.1 Premortem account sharing. Premortem sharing of account access—either directly (e.g., sharing passwords, joint account ownership, giving power of attorney, providing remote access) or indirectly (e.g., sharing the location of documents containing account passwords)—was common. Most of the time, premortem sharing was not expressly intended for postmortem account access, but rather for convenience. Participants sometimes found online account management difficult, and shared account access so that heirs could help manage certain aspects of online accounts. Nonetheless, participants felt that existing premortem sharing practices can easily translate to postmortem account access and management. This reduces burden both premortem on account holders for account management, as well as postmortem on heirs, who already have access to these accounts. Almost all participants engaged in premortem sharing and explicitly stated that they trusted their heirs not to take inappropriate actions, even on sensitive accounts (e.g., financial, email).

4.3.2 Leveraging existing password-management practices for digital estate planning. Beyond premortem sharing, participants reported leveraging practices they already use to handle postmortem account access. All participants primarily used manual methods to keep track of their online accounts: most participants used pen-and-paper to manage their passwords and kept paper copies of their account information and passwords somewhere in their home. About half had digital files of their passwords, with paper backups. Most participants also used password managers for some passwords—sometimes without realizing—and said heirs could utilize the passwords stored on their devices or browsers to access their digital accounts after their passing, but noted these records are incomplete. A few participants expressed concerns about digital security and said they never digitally save passwords to high-risk accounts (e.g., banking). These participants noted their heirs would need access to their physical copy of passwords to gain access to those high-risk accounts.

Participants preferred physical pen-and-paper systems for both premortem and postmortem credential sharing because they felt confidence in the security and in their understanding of the mechanism. Many expressed trust in the (physical) security of their password-management practices, noting that if someone was able to enter the space in which the passwords document was kept, it was likely to be someone that they already trusted with that information. A few participants mentioned that a physical copy of their passwords was in a safe deposit box that heirs would have access to after their death. Almost all participants felt that having access to the existing paper document or digital file would be sufficient for executors and heirs to access whichever accounts were necessary, with or without explicit instruction. Many participants had informed heirs of the location of these files.

While keeping all passwords in one place (e.g., notebook) that heirs know about reduces the need to piece together account access information, this practice also appears in tension with participants' consideration of easing the burden on heirs during postmortem digital estate planning (§ 4.2.3). Although a few participants said that they marked accounts that needed the most attention (e.g., financial accounts)—and some stated they had few accounts and so the burden on heirs should be low—the majority of participants had not thought about how their existing practices could create a burdensome postmortem management process, when files with dozens or hundreds of account credentials are passed down.

4.3.3 Online accounts are often not part of formal processes. While most participants had gone through estate planning processes, only a few had formal provisions for online accounts, e.g., designating them as part of a will or trust. Online accounts had generally not been considered during the estate planning process when participants initially discussed estate planning 8 to 30 years ago. Even Carol, who updated her will in the last year, did not recall discussing online accounts. As she noted, "The lawyer is probably pretty much my age, or a little bit younger. ... We didn't grow up with computers. So it's not in our thinking."

While estate planners may not routinely bring up online accounts, some participants reported hearing about the need for planning around digital assets from friends or media articles. Michael mentioned that the impetus for including online accounts was due to hearing from friends who had included such information in their estate plan. Charles encountered information online in a news article that suggested creating a "big book" that included relevant legal documents, as well as instructions for heirs, including for digital assets [25]. The information regarding online accounts nonetheless were not legally formalized, but were easily accessible for heirs.

Even though postmortem account access considerations tend to fall by the wayside in the formal estate planning process, participants nonetheless all had *ad-hoc* and informal means to ensure heirs have access to those online accounts. These practices are based on their existing credential-management practices, such as passing down passwords or pointing heirs to the locations where account credentials were stored.

4.4 Digital Estate Planning Barriers and the Preference for Familiar Non-Technical Approaches

Participants' most prevalent concerns about postmortem account access were those unique to digital estates, such as about password management or about security and usability. Though most participants thought technical tools such as password managers or legacy features could be more convenient for managing their digital estate, most still preferred approaches that they already used and were familiar with, even if imperfect. Participants also mentioned concerns around estate planning more generally, such as emotional challenges. Meanwhile, only a few participants brought up privacy or legality as potential concerns for digital estate planning.

4.4.1 Keeping records of accounts and passwords up to date and relevant. Most participants found the ongoing management of accounts and passwords tedious due to requirements to change passwords periodically. Almost all participants expressed frustration about keeping records of their passwords up to date. A few noted that updating passwords written down on paper can be tedious and messy, and that sometimes the documents would run out of space. Other participants had a digital file of passwords, which may be easier to update, but they still struggled with making sure that executors knew where the most updated files are on a regular basis. Carol explained, "I hadn't even thought about giving [a password] to the attorney mainly because it might change before I die, and it would be the wrong one."

Difficulties in keeping passwords lists up to date led a few participants to adopt password managers. Other participants said they much prefer to write passwords down on paper, in some cases due to inaccurate perceptions that password managers are insecure [50]. Participants felt that being able to just share one password with heirs was convenient, if all other passwords were automatically kept up to date in the password manager, but security concerns sometimes outweighed the perceived benefits of that convenience.

Some participants were reluctant to burden heirs with large numbers of accounts, including many that they no longer used. While most participants wanted to select which accounts or data (e.g., photos) to share or transfer, the sheer number of accounts and amount of data made it difficult to determine how to organize this process. About half of participants said that they gave, or indicated that they would give, their executor access to all their passwords and data rather than making selections. Frances said she would "share everything with them and let them figure it out." Similarly, Barbara explained, "I wouldn't pick and choose. [My heir] would get all or nothing." This speaks to assumptions held by participants that heirs would figure out intuitively what accounts are important rather than leave instructions, even if those participants also wanted to reduce the burden on their heirs.

Meanwhile, to reduce the burden on their heirs, some participants explicitly mentioned a desire to delete accounts they no longer used.

> I do the heavy lifting on this stuff because I'm alive. But when I die, somebody else has got to basically step into that role. –*Charles*

Irene wanted to clean up her accounts, but said she was unlikely to actually do it: "Ideally, I should go through all of those accounts and figure out which to 'kill' myself right now. Will I do that? ... Probably not unless I'm really bored one day." While it would reduce burdens on heirs to manage fewer accounts, the tedium and burden on the account holder pose non-trivial barriers.

4.4.2 Concerns about using technology. While most participants said that technical tools such as password managers and legacy account features sounded useful, many were concerned that they would be difficult to use and some had already encountered challenges using them. These encountered or perceived barriers may prevent older adults from trying out or adopting tools that may be helpful and lead them to default to practices that they were confident they could use, such as keeping pen-and-paper records.

> I find even simple things on the computer get complicated and they're hard for me. So I try to avoid computer stuff as much as I can. ... I'd be willing to give it a try, but I think I would give up fast if it took a lot of effort. –*Gloria*

A few participants also mentioned that they had not adopted password managers due to concerns that transferring their passwords from paper to a password manager would be difficult and time consuming. Similar to concerns with other technologies, participants expressed uncertainty on how password managers function and concerns that misconfigurations or errors would compromise or delete their passwords.

> [Password managers] seems vulnerable from security, and it seems there's a good likelihood that I would somehow mess it up, and [my passwords] would be gone forever. ... So I will never do that. –*Gloria*

In contrast to what was found in prior work, privacy concerns were not prevalent among our participants [9, 11, 26]. More specifically, most participants were unconcerned about sharing account passwords or data such as photos or personal mementos with heirs. This sanguine attitude towards sharing data also is demonstrated in the premortem sharing of account credentials and contents with inheritors. However, participants stated that the data was intended only for that specific audience and they had privacy concerns regarding the spread of data beyond their designated inheritors. Some participants were reluctant to use technical tools due to uncertainty about how they work and fears of "messing it up" and accidentally exposing data to an audience beyond what they intended due to incorrectly configuring tools.

Most participants also expressed concerns about the security of data in online accounts or of credentials in passwords managers. Most were worried about data breaches or hackers, though few

explained what specific harm they feared from hackers. One participant explicitly mentioned potential reputational harms from hackers that take over accounts, such as to send spam. Edward identified AI as a potential concern due to the possibility of data misuse and being uncertain about what might happen with data or inferences that could be made if an AI system was trained on his data. Many participants recounted reading stories or receiving notifications about account breaches and credential leaks. Others described their own experiences with hacks or credential theft. No participants expressed security concerns in sharing account information with heirs—all of whom are adults—though a few mentioned not wanting grandchildren who are teenagers or younger to have access.

Despite stated concerns, most participants used the password managers built into their OS or web browser—sometimes without thinking of them as password managers. Participants also tended to be less worried about passwords that they believed to be stored locally. In fact, a few participants had the (mis)perception that passwords in browser based-password managers were stored locally, which provided some assurance to them about digital security. Similar to what was reported in previous work [50], a few participants were particularly concerned about using third-party password managers, despite the fact that password managers can actually help users avoid some types of attacks. A few participants who used password managers explicitly stated that they never saved the passwords for important accounts, such as financial accounts, but were fine with saving other passwords. This suggests that despite a lack of trust in password managers, participants but will use them out of convenience for accounts where they do not see much risk. However, given this mistrust, the financial accounts that participants believed most important to pass on would not be included. Thus, while participants were interested in using technical tools like password managers for convenience in their existing credential management and for credential sharing, they are often hindered by mistrust—both of the technology and their own abilities.

4.4.3 Emotional challenges. While participants were comfortable talking about death and estate planning to participate in our study, many still found end-of-life planning to be unpleasant. Carol explained, "It's something that's not fun to do, and you have to.... It's hard to sit down and make yourself do things you don't like to do." Combined with the tedium of managing and sorting through the large numbers of online accounts to filter out those that are inactive, these barriers make it difficult for participants to actually find the time or motivation to take these actions, despite knowing their importance for reducing burden on heirs.

Although all the older adults we interviewed were sanguine about end-of-life planning, the emotional toll of digital estate planning may still pose a barrier. In particular, the act of designating legacy contacts for online accounts was a choice that was emotionally fraught for a few participants. Furthermore, a few participants noted that their heirs or executors were not always comfortable having conversations that were necessary to convey information about postmortem account management, for example sharing the location of documents and passwords, or expectations surrounding accounts.

4.5 What Would Make Digital Estate Planning Easier

We found no specific approaches for digital estate planning that were universally liked or disliked by participants. Preferences varied by type of account, and different participants sometimes expressed opposing views. Participants were particularly interested in potential ways to determine the granularity of data shared as well as customizing timing for notifying heirs or shutting down accounts. We first discuss results about legacy features and potential extensions (§4.5.1), then new features that could offer convenience and organization (§4.5.2), and, finally, expert guidance for digital estates (§4.5.3).

4.5.1 Digital legacy features. Most participants were interested in learning more about digital legacy features and inactive account managers provided by Facebook, Apple, or Google and believed that these features could simplify digital estate planning and reduce the burden on heirs. Only a few participants had used these features themselves, while most participants were unaware of these features before the interviews.

While Google's Inactive Account Manager is primarily intended for sharing content from Google Accounts after a period of inactivity, participants were most curious about the notification that the feature sends out after inactivity rather than the sharing of data within the account, revealing a gap between what such tools intend to do with what older adults need. Participants had further questions and suggestions for notifications—expanding beyond Google Accounts—as well as questions about customization of message and timing.

Participants felt that notifications for inactive accounts needed to be appropriately timed and the desired timing varied by participant and use case. Irene said she did not want the notification to go out after a week of inactivity when she might be at the hospital undergoing surgery. Other participants did not want the time of inactivity to be too long, as the sudden arrival of a notification to their loved ones a few months after the death of the account owner may cause further grief. Linda also raised concerns that data may be deleted too quickly while heirs still needed access.

Participants also imagined a variety of notification-related features that they would find useful, built into the account either as part of account creation or general use. Some envisioned an inventorying tool—a way of notifying heirs about the existence of accounts that may need to be managed or closed down. These envisioned features were to allow heirs to manage accounts and so that heirs had control over deciding what data to keep or delete. Others wanted to be notified every so often to review the trusted contact information they registered previously and update it if necessary.

> A pop up asking if there's a trusted contact. You put in the information [of the trusted contact] ... and every once in a while the account sends a reminder, [and asks], is this still your trusted contact and email? There is a good reminder to update if needed. – *Arthur*

The automatic closure of inactive accounts with legacy features was alternatively seen as a benefit or drawback by different participants. Some participants liked automatic account closures due to

placing the burden on the platforms themselves to manage accounts rather than on the bereaved. However, other participants felt that automatic account closures reduced their control and could result in loss for accounts with monetary value. They did not want bank or travel reward accounts to be automatically closed—although such types of accounts generally do not currently have features that would automatically close the accounts. Some participants felt that for less important accounts, automatic account closure would be useful as a means of dealing with large numbers of accounts without requiring action from heirs or executors, also addressing the desire to minimize burden on heirs. Even if participants shared credentials for all accounts, heirs do not need to take action on accounts that automatically close, potentially resolving a tension between those desires. The idea of having a notification to the account owner or designated contact before shutting down the account was also appealing. However, one participant was concerned that account notifications could leak private information about the deceased's interests, such as for shopping accounts.

4.5.2 New technical tools and features. Some participants wanted control over which specific accounts or data (e.g., photos) to share, while others were comfortable providing access to everything stored in all of their accounts. Some participants expressed interest in features that could provide granular account management, which current tools often lack. For example, Google Inactive Account Manager does not allow for sharing of select photos or selected emails.[3]

Irene wanted the ability to share particular folders of photos with heirs rather than all the photos in her account: "Probably some of my photos are grouped into folders, so I can probably narrow it down to folders within there." About half of the participants were more interested in using granular control to reduce the burden on inheritors than to protect their own privacy. Participants did not want inheritors to have to wade through gigabytes of photos or files that they deemed to be irrelevant or uninteresting. These participants envisioned granular control features that allowed them to manage their data now, so that after their passing only memories they felt were worthwhile are shared. However, this would be time consuming and tedious, and participants stated that they would not prioritize such tasks.

On the other end of the scale from granular control, a few participants envisioned a centralized method of postmortem account management that would allow them to set preferences for all accounts of a particular type rather than having to manage individual accounts. Participants wondered whether password managers could be a way to facilitate this management.

4.5.3 Expert guidance. A few participants mentioned wanting an expert to answer their questions about digital estate planning, or guide them through setting up account management systems, legacy features, or password managers, and thought it would be helpful in both pre- and postmortem digital estate management. Donna explained, "It would be nice if I had somebody to sit here beside me ... and set legacy features up." Some participants were interested in using password managers to aid in digital estate planning, particularly for convenience, while others were wary of password managers and raised security concerns. Expert guidance and workshops were seen as potential avenues to explore password managers both for those interested in the tool as well as for skeptics who wanted reassurance.

> I was working with a a digital team that gave me training on how to use these tools...[and] help me set up 1password. –*Alice*

Participants often had questions about password managers, and mentioned wanting to examine password managers more before committing to using them. Elizabeth wanted to be able to use other methods of organizing her passwords as a backup rather than relying solely on the password manager. She wondered, "Would I have the ability to print that stuff out as a backup? Would I be able to give access to that to my spouse or son? You know, how would that work?"

Participants who were less confident in their technical ability said they would be more comfortable using tools and features under expert guidance. Indeed, many participants mentioned that they had gained confidence in using certain systems or managing their online accounts after learning from knowledgeable friends or family. Beyond professionals and experts, family members who were deemed tech-savvy were often pinpointed as possible resources to help with management of online accounts and digital estates.

5 Discussion

Drawing upon our findings, we discuss potential interventions for practitioners and online platforms to better facilitate digital estate planning for older adults. We suggest moving beyond digital legacy—primarily focused on data—to the digital estate—digital assets and digitally-enabled physical assets and accounts [10]. This frames online accounts as part of a digital and physical ecosystem rather than as isolated pieces, and better allows those conducting digital estate planning to evaluate accounts in terms of overall value beyond the data they contain. We offer recommendations based on our observations of what is currently missing in digital estate planning for older adults, what challenges are present, and propose steps towards establishing future standards to support digital estate planning across a larger population of users.

5.1 Challenges and Gaps Stemming from Existing Practices

Our results suggest that while older adults are invested in managing their digital estates and planning for postmortem transfer of their accounts, their practices and expectations do not always align well with their desired outcomes (§4.2 and §4.3). While most participants claimed to have fairly comprehensive traditional estate plans, digital estate planning presented challenges (§4.4).

All participants stated an overarching desire to reduce the burden of closing out their digital estate (§4.2.3). Other considerations and practices were sometimes at odds with that desire. Participants planned to share all their passwords with heirs and assumed heirs would be able to figure out what to do (§4.2.2). However, going through long lists of credentials may in fact be difficult without further instructions about the account holder's expectations for each account (§4.3.2). Indeed, participants themselves noted that it was difficult for them to sort through their own accounts. However,

[3] https://support.google.com/accounts/answer/3036546?hl=en

if account holders do not pass down account credentials, there may not be legal recourse for their heirs to gain access to the accounts.

Despite participants mentioning that tools such as legacy features or password managers would be helpful both for themselves and heirs, security concerns or wariness of technical misconfigurations hinder adoption (§4.4.2). Participants also noted different preferences for what to share—some wanted granular control over what to pass on to heirs, while others took an all or nothing approach for accounts and data (§4.5.2). Given these tensions, we propose recommendations based on our study to ease digital estate planning for older adults, reduce burden for heirs, and resolve some tensions between the stated needs of participants and their current practices.

5.2 Learning from Traditional Estate Planning for the Digital Realm

Older adults would benefit from approaches that leverage their existing credential management practices (§4.3.2) and present digital estate planning in terms analogous to traditional estate planning rather than focusing on digital legacy and data [7, 11, 19, 32, 45]. Expert guidance in planning can make the process easier, and provide the support necessary for older adults to properly set up legal instructions and technical tools, further reducing barriers (§4.5.3).

Recommendation 1: Leverage familiar credential management and estate planning practices. Even when participants felt that technical tools would be useful, concerns about security and their own technical abilities hindered adoption. Participants often preferred familiar physical methods of account management that they felt confident they understood. Using concepts from traditional estate planning as an overarching known metaphor for digital estate planning could provide reassurance, self-efficacy, and reduce concerns about technical tools.

A first step in traditional estate planning is often an inventory of assets. Prior work has found this initial inventorying of online accounts for digital legacy planning to be a hurdle [11]. Meanwhile, the current approaches to account management mentioned by participants—e.g., documents that list all accounts and passwords—already result in a fairly complete inventory. These documents (or, equivalently, password managers) can be an opportunity for starting the process of digital estate planning, rather than starting from scratch.

People could be encouraged to categorize their accounts in their paper lists or password managers to facilitate digital estate planning, for example, in terms of value, whether monetary, sentimental, or practical—similar to how assets with monetary and sentimental value are accounted for in traditional estate planning. People could also be encouraged to annotate their password lists with instructions about whether and with whom account credentials should be shared and any actions that should be taken with each account. Making a distinction between passing on purely digital assets and passing on digital access to physical assets and accounts could help make the process less daunting. Digital assets might be transferred to heirs, and accounts shut down automatically, without the need to transfer credentials for accessing those accounts. Account owners would then have a smaller set of accounts that have credentials they would need to transfer so that heirs could take actions, such as making payments or cancelling subscriptions. Providing clear instructions along with credentials would reduce the burden on heirs.

Categorizing and annotating accounts as they are added and updated in existing management systems could reduce the need to sort through large numbers of accounts during the estate planning process and for heirs during postmortem management.

Recommendation 2: Offer expert guidance through professionals or guides developed by experts. Participants were interested in expert guidance to assist with their digital estate planning, echoing prior work that found human-facilitated sessions to be useful when doing such planning [11]. Ideally, estate-planning professionals older adults already work with could offer support on digital estate planning or refer clients to experts. Workbooks and checklists developed by experts can reveal gaps those undertaking digital estate planning might otherwise miss.

Prior to the interview, most participants had not considered account dependencies, such as a phone number being required for 2FA or an email account being needed for account-recovery. Such dependencies between accounts are crucial for how heirs order their management of account closures. Expert guidance could help older adults realize the importance of account dependencies and thus provide better instructions to their heirs.

Experts could guide and make suggestions about how to leverage current credential management, as well as recommend alternative approaches. Legal professionals could provide assistance in setting up power-of-attorney or designating instructions that comply with RUFADAA to give fiduciaries or designated recipients legal authority to manage or access digital assets, formalizing both pre- and postmortem access to accounts [58]. Experts can also guide older adults in setting up technical features and providing reassurance on digital security and correct setup. Aid in using these features could reduce the burdens on older adults who are hesitant to try out technological features.

5.3 Technical Features for Postmortem Account Management

Digital legacy features such as those provided by Apple, Google, and Facebook provide alternative means beyond sharing passwords that allow heirs to access (and sometimes manage) data in online accounts [4, 18, 39]. Most participants showed interest in these features and their functionalities (§4.5.1). Unfortunately, these features were not well-known to participants prior to the interviews. Further, none of the existing features fully encapsulate the needs elicited from our interviews, nor were they available for all the accounts that participants wanted them for. For example, some participants wanted accounts to have automatic closures, such as Google's Inactive Account Manger, while other preferred heirs taking some action when the time was right to access the account, such as with Apple's Legacy Contact feature. Some participants expected the ability to choose what contents of the accounts to share, while others felt no need to curate what was passed on. In addition, many legacy features provide access to the contents of accounts, but often have limited account management access. Given these differing expectations between different participants as well as between what participants wanted and what is offered,

we discuss design principles that would allow for customization while providing ease of use and address the needs of older adults as expressed by our participants.

Recommendation 3: Standardize digital legacy features with usability in mind. We recommend that digital legacy features be standardized across platforms to facilitate digital estate planning and centralize management of accounts. Rather than a patchwork of features, each implemented differently by the respective platforms, standardized legacy features that use consistent terminology could make digital estate management easier. This would make it easier for account holders to find and configure legacy features for all of their accounts and even facilitate the creation of legacy configuration dashboards. Future work could investigate which specific features or terms are most usable across user needs and account types.

Recommendation 4: Control over notification timing and message for inactive accounts. Notifications of account inactivity could be customized to suit the needs of the account holder. Notifications could alert heirs to the presence of accounts that may have been missed during the close out of the digital estate, inform contacts that an account is no longer active, provide a selected highlight of cherished photos or memories that account holders wanted to share, or remind heirs to save important data prior to automatic account shutdown. Participants wanted certainty that notifications would not be sent too early, when they still are using the account, nor too late, such that it would be a shock for recipients or too much of a lag for adequate postmortem account management.

A standardized, customizable notification feature would allow account holders to specify the messages and recipients for each account as well as the length of "inactivity" prior to notification. This echoes findings from prior work of the importance of personalization [9, 56]. Future work could determine which categories of notification types and timing granularities would be most useful and explore the possibility of a staged notification process where a smaller number of trusted contacts might be asked whether inactivity is due to a temporary absence before additional notifications go out or accounts are shut down.

Recommendation 5: Automatic account shutdowns and default actions for accounts. Automatic actions (such as account deletion) after a certain amount of inactivity could reduce burden on account holders and heirs, potentially reducing the number of accounts that need manual management, addressing a concern that participants raised. These actions could be set by default, or defining postmortem contingencies could be a required part of account setup. This could reduce the burden of having to manage and decide what to do with dozens or hundreds of accounts at once when inventorying. In some cases, account holders might specify actions to be taken prior to account shutdown, such as transferring data or assets from the account to designated heirs. While account defaults may reduce burden, prior work has noted that chosen defaults may be "easy" but not properly reflect the full desires of users [11, 26]. Thus, accounts could have periodic notifications for users to check or update these settings. Automatic closure may not be appropriate for accounts that heirs may need in order to take actions and gain access to other accounts. Since this is a complicated matter on which participants' preferences diverged, we encourage future research to investigate best practices for automatic account management options.

5.4 Limitations

As our study was advertised as an interview on digital estate planning, our sample may be biased toward individuals who were interested in and comfortable talking about the topic. Because of the difficulty of recruiting participants for a study that explored potentially sensitive or uncomfortable topics, we recruited via personal contacts, via physical posters, mailing lists for older adult continued education programs, and snowball sampling. The snowball sampling and personal contacts may have reduced the diversity of our sample. While the population we recruited is not representative of older adults from every walk of life, we attempted to diversify our recruited sample to the extent possible and share participants' demographics in Table 1.

All participants who completed our study had at least US $100K in assets, limiting our findings' applicability to older adult with under US $100K in assets. For context, the median household net worth for people 65–74 years old in the U.S. in 2022 was US $410K [14]. The range of valuations of the assets of participants in our sample was otherwise broad, and we observed no obvious trends related to the value of assets.

Our findings are qualitative and aimed at exploring how older adults manage their online accounts, rather than providing quantitative evidence about broader population-level digital estate planning practices. Additionally, all participants had either executed or considered formal or informal methods of sharing account access with heirs, which may limit the diversity of perspectives captured. As is common in interview studies, detailed analysis gives rise to new questions that cannot be answered by the data at hand. Given the limitations of our work, we suggest that future work could examine individuals who have not yet considered digital estate planning, including, in particular, younger populations who may hold a greater number of online accounts and face different challenges and attitudes toward digital estate management. Our research focused on the U.S. context; we encourage future work to examine contexts outside the U.S. to understand where preferences or needs may diverge. We also recommend future work to examine which specific features and standards (such as notification systems and account defaults) would be most useful and usable across users, assets, and account types.

6 Conclusion

While older adults more often engage in traditional estate planning, these processes may not formally address the novel challenges that arise from planning for digital estates, including both digital assets and accounts that provide access to non-digital assets. We conducted semi-structured interviews with 21 older adults and found that participants' approaches to providing heirs access to their digital estates are primarily informal and leverage their existing credential-management practices. Accounts with access to monetary assets were the only ones consistently prioritized by all participants. Participants trusted inheritors and executors to not take inappropriate actions with sensitive accounts (such as banking

or email) and often shared account access premortem, envisioning that this would provide for continued access postmortem. We also found tensions between participants' practices and desired outcomes for heirs, e.g., the practice of keeping all passwords in one file clashes with the desire to reduce burden on heirs by only passing on credentials needed for key accounts. Despite frustrations with pen-and-paper approaches for managing large numbers of online accounts, concerns about technical ability hindered adoption of technological methods (e.g., legacy features, password managers) that could aid in digital estate planning. Preferences for tools varied, with timeliness and ease of use for older adults and for heirs surfacing as major considerations. Finally, participants also valued non-technical support, such as having experts guide them through the process of digital estate planning and credential management. Based on our findings, we made five recommendations for digital estate planning and suggest future research to explore the digital estate planning needs across broader populations.

References

[1] Andrew A Adams and Shirley A Williams. 2014. What's yours is mine and what's mine's my own: joint accounts and digital identity. *ACM SIGCAS Computers and Society* 44, 1 (2014), 15–26.

[2] Social Security Administration. 2025. *Top names of the 1940s.* Retrieved 2025-05-13 from https://www.ssa.gov/oact/babynames/decades/names1940s.html

[3] Nora Alkaldi and Karen Renaud. 2016. Why do people adopt, or reject, smartphone password managers?. In *1st European Workshop on Usable Security-EuroUSEC 2016*. Internet Society, Darmstadt, Germany.

[4] Apple. 2024. *How to add a Legacy Contact for your Apple Account.* Retrieved 2025-05-13 from https://support.apple.com/en-us/102631

[5] J. D. Biersdorfer. 2025. *How to Prepare for Your Digital Afterlife.* Retrieved 2025-09-10 from https://www.nytimes.com/2025/02/12/technology/personaltech/social-media-accounts-death.html

[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[7] Jed R. Brubaker, Lynn S. Dombrowski, Anita M. Gilbert, Nafiri Kusumakaulika, and Gillian R. Hayes. 2014. Stewarding a legacy: responsibilities and relationships in the management of post-mortem data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 4157–4166. doi:10.1145/2556288.2557059

[8] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 117–136. https://www.usenix.org/conference/soups2019/presentation/busse

[9] Janet X. Chen, Francesco Vitale, and Joanna McGrenere. 2021. What Happens After Death? Using a Design Workbook to Understand User Expectations for Preparing their Data. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 169, 13 pages. doi:10.1145/3411764.3445359

[10] Dylan Thomas Doyle and Jed R Brubaker. 2023. Digital legacy: a systematic literature review. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–26.

[11] Dylan Thomas Doyle and Jed R. Brubaker. 2024. "I Am So Overwhelmed I Don't Know Where to Begin!" Towards Developing Relationship-Based and Values-Based End-of-Life Data Planning Approaches. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 219, 14 pages. doi:10.1145/3613904.3642250

[12] Lilian Edwards and Edina Harbina. 2013. Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Ent. LJ* 32 (2013), 83.

[13] Farida Eleshin, Qi Sun, Mengzhe Ye, Sauvik Das, and Jason I. Hong. 2025. Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management among Cryptocurrency Users. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 921, 19 pages. doi:10.1145/3706598.3713209

[14] Fidelity. 2025. Average and Median Net Worth by Age. https://www.fidelity.com/learning-center/smart-money/average-net-worth-by-age

[15] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 21–40. https://www.usenix.org/conference/soups2019/presentation/frik

[16] Katie Z Gach and Jed R Brubaker. 2020. Experiences of trust in postmortem profile management. *ACM Transactions on Social Computing* 3, 1 (2020), 1–26.

[17] Katie Z Gach and Jed R Brubaker. 2021. Getting your Facebook affairs in order: User expectations in post-mortem profile management. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–29.

[18] Google. 2025. *About Inactive Account Manager - Google Account Help.* Retrieved 2025-05-13 from https://support.google.com/accounts/answer/3036546?hl=en

[19] Rebecca Gulotta, David B. Gerritsen, Aisling Kelliher, and Jodi Forlizzi. 2016. Engaging with Death Online: An Analysis of Systems that Support Legacy-Making, Bereavement, and Remembrance. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 736–748. doi:10.1145/2901790.2901802

[20] Rebecca Gulotta, William Odom, Haakon Faste, and Jodi Forlizzi. 2014. Legacy in the age of the internet: reflections on how interactive systems shape how we are remembered. In *Proceedings of the 2014 Conference on Designing Interactive Systems* (Vancouver, BC, Canada) *(DIS '14)*. Association for Computing Machinery, New York, NY, USA, 975–984. doi:10.1145/2598510.2598579

[21] Rebecca Gulotta, William Odom, Jodi Forlizzi, and Haakon Faste. 2013. Digital artifacts as legacy: exploring the lifespan and value of digital data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 1813–1822. doi:10.1145/2470654.2466240

[22] Betsy Simmons Hannibal. 2025. *The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA).* Retrieved 2025-09-10 from https://www.nolo.com/legal-encyclopedia/ufadaa.html

[23] Edina Harbinja. 2019. Emails and death: Legal issues surrounding post-mortem transmission of emails. *Death Studies* 43, 7 (2019), 435–445.

[24] Amelia Hassoun, Ian Beacock, Sunny Consolvo, Beth Goldberg, Patrick Gage Kelley, and Daniel M. Russell. 2023. Practicing Information Sensibility: How Gen Z Engages with Online Information. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 662, 17 pages. doi:10.1145/3544548.3581328

[25] Thomas Heath. 2018. *Let's talk about the Big Book: Everything your family needs to know when you die.* Retrieved 2025-05-13 from https://www.washingtonpost.com/business/economy/its-that-time-of-year-lets-talk-about-the-big-book/2018/05/18/da00f2f8-5932-11e8-8836-a4a123c359ab_story.html

[26] Jack Holt, James Nicholson, and Jan David Smeddinck. 2021. From Personal Data to Digital Legacy: Exploring Conflicts in the Sharing, Security and Privacy of Post-mortem Data. In *Proceedings of the Web Conference 2021* (Ljubljana, Slovenia) *(WWW '21)*. Association for Computing Machinery, New York, NY, USA, 2745–2756. doi:10.1145/3442381.3450030

[27] Jamie P Hopkins. 2013. Afterlife in the cloud: Managing a digital estate. *Hastings Sci. & Tech. LJ* 5 (2013), 209.

[28] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[29] Maria Karyda, Elisa D Mekler, and Andrés Lucero. 2021. Data Agents: Promoting Reflection through Meaningful Representations of Personal Data in Everyday Life. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 367, 11 pages. doi:10.1145/3411764.3445112

[30] Samantha Murphy Kelly. 2024. *We each have an average of 100 online accounts. Here's how to make sure they aren't a nightmare for your family if you die.* Retrieved 2025-09-10 from https://www.cnn.com/2024/02/26/tech/digital-legacy-planning-personal-technology/index.html

[31] Junchao Lin, Jason I Hong, and Laura Dabbish. 2021. " It's our mutual responsibility to share" The Evolution of Account Sharing in Romantic Couples. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–27.

[32] Michael E. Locasto, Michael Massimi, and Peter J. DePasquale. 2011. Security and privacy considerations in digital death. In *Proceedings of the 2011 New Security Paradigms Workshop* (Marin County, California, USA) *(NSPW '11)*. Association for Computing Machinery, New York, NY, USA, 1–10. doi:10.1145/2073276.2073278

[33] A. Lowik, J. J. Cameron, J. Dame, J. Ford, L. Pulice-Farrow, T. Salway, S. van Anders, and K. Shannon. 2024. *Gender & Sex in Methods & Measurement – Research Equity Toolkit: Tool #9: Qualitative Considerations.* Technical Report. Collaborative of Gender and Sexual Health Equity Research Education Resources (CGSHE), University of British Columbia, Vancouver, BC, Canada. https://cgshe.ca/app/uploads/2019/11/GSMM-T9-FINAL.pdf

[34] Cristiano Maciel and Vinicius Carvalho Pereira. 2015. Post-mortem Digital Legacy: Possibilities in HCI. In *Human-Computer Interaction: Users and Contexts*, Masaaki Kurosu (Ed.). Springer International Publishing, Cham, 339–349.

[35] Michael Massimi, William Odom, Richard Banks, and David Kirk. 2011. Matters of life and death: locating the end of life in lifespan-oriented hci research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 987–996. doi:10.1145/1978942.1979090

[36] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5921–5932. doi:10.1145/2858036.2858051

[37] Nora McDonald, Alison Larsen, Allison Battisti, Galina Madjaroff, Aaron Massey, and Helena Mentis. 2020. Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Virtual, 99–110. https://www.usenix.org/conference/soups2020/presentation/mcdonald

[38] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[39] Meta. 2025. *About legacy contacts on Facebook | Facebook Help Center.* Retrieved 2025-05-13 from https://www.facebook.com/help/1568013990080948

[40] Johan David Michels, Sharon Hartung, and Christopher Millard. 2021. *Digital Assets: A Call To Action.* Technical Report. Queen Mary University of London, The Society for Trust and Estate Practitioners, United Kingdom. https://ssrn.com/abstract=3925439

[41] Johan David Michels, Dimitra Kamarinou, and Christopher Millard. 2019. *Beyond the Clouds, Part 2: What Happens to the Files You Store in the Clouds When You Die?* Technical Report. Queen Mary University of London, United Kingdom. https://ssrn.com/abstract=3387398

[42] Johan David Michels, Christopher Millard, and Srishti Joshi. 2019. *Beyond the Clouds, Part 1: What Cloud Contracts Say About Who Owns and Can Access Your Content.* Technical Report. Queen Mary University of London, United Kingdom. https://ssrn.com/abstract=3386609

[43] Stephanie Mlot and Jason Cohen. 2024. *How to Prepare Your Digital Life for Your Death.* Retrieved 2025-09-10 from https://www.pcmag.com/how-to/how-to-prepare-your-digital-life-accounts-for-your-death

[44] Phoebe Moh, Andrew Yang, Nathan Malkin, and Michelle L. Mazurek. 2024. Understanding How People Share Passwords. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 219–237. https://www.usenix.org/conference/soups2024/presentation/moh

[45] Wendy Moncur and David Kirk. 2014. An emergent framework for digital memorials. In *Proceedings of the 2014 Conference on Designing Interactive Systems* (Vancouver, BC, Canada) *(DIS '14)*. Association for Computing Machinery, New York, NY, USA, 965–974. doi:10.1145/2598510.2598516

[46] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. The Burden of Ending Online Account Sharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376632

[47] William Odom, Richard Banks, David Kirk, Richard Harper, Siân Lindley, and Abigail Sellen. 2012. Technology heirlooms? considerations for passing down and inheriting digital materials. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 337–346. doi:10.1145/2207676.2207723

[48] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. 2023. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 864, 21 pages. doi:10.1145/3544548.3580766

[49] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and share alike? an exploration of secure behaviors in romantic relationships. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 83–102.

[50] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 319–338. https://www.usenix.org/conference/soups2019/presentation/pearman

[51] Haley Perry. 2025. *A Loved One Dies. No One Knows Their Passwords. Here's What to Do.* Retrieved 2025-09-10 from https://www.nytimes.com/wirecutter/reviews/advice-password-recovery-after-death/

[52] Joachim Pfister. 2017. "This will cause a lot of work.": Coping with Transferring Files and Passwords as Part of a Personal Digital Legacy. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 1123–1138. doi:10.1145/2998181.2998262

[53] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Virtual, 73–90. https://www.usenix.org/conference/usenixsecurity21/presentation/ray

[54] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '07)*. Association for Computing Machinery, New York, NY, USA, 895–904. doi:10.1145/1240624.1240759

[55] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I Hong, and Laura Dabbish. 2019. Normal and easy: Account sharing practices in the workplace. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–25.

[56] Lisa Thomas and Pam Briggs. 2014. An older adult perspective on digital legacy. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational* (Helsinki, Finland) *(NordiCHI '14)*. Association for Computing Machinery, New York, NY, USA, 237–246. doi:10.1145/2639189.2639485

[57] Trust & Will. 2025. Redefining Legacy. https://trustandwill.com/documents/2025-estate-planning-report 2025 Estate Planning Report.

[58] Uniform Law Commission. 2015. Revised Uniform Fiduciary Access to Digital Assets Act. Approved by the National Conference of Commissioners on Uniform State Laws. https://www.uniformlaws.org/committees/community-home?communitykey=f7237fc4-74c2-4728-81c6-b39a91ecdf22 Uniform Act.

[59] Lirong Yuan, Yanxin Chen, Jenny Tang, and Lorrie Faith Cranor. 2024. Account password sharing in ordinary situations and emergencies: A comparison between young and older adults. In *USENIX Symposium on Usable Privacy and Security (SOUPS) Poster Session*. USENIX Association, Philadelphia, PA.

[60] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. 2024. Cross-contextual examination of older adults' privacy concerns, behaviors, and vulnerabilities. *Privacy-Enhancing Technologies (PoPETs)* 2024 (2024), 133–150.

A Interest Survey

[Informed Consent]

Consent Questions

- I have read and understood the information above.
  - Yes
  - No
- I am age 60 or oder.
  - Yes
  - No
- I am located in the United State.
  - Yes
  - No
- I am fluent in English.
  - Yes
  - No
- I want to participate in this research and continue with the survey.
  - Yes
  - No

Demographics Questions

- What is your age?
  [text box]
- What is your gender?
  - Male
  - Female
  - Non-binary
  - Prefer to self describe [text box]
- How would you describe your race? Please select all that apply.

  - White
  - Black or African American
  - Native American or Alaska Native
  - Asian
  - Native Hawaiian or Pacific Islander
  - Other [text box]
- What is your total net worth (total assets minus total liabilities)?
  - Less than $100,000
  - $100,000 – $1,000,000
  - $1,000,000 – $5,000,000
  - $5,000,000 – $30,000,000
  - $30,000,000 or more
  - Prefer not to say
- Do you have a will?
  - Yes
  - No
  - Other [text box]
- Which, if any, of these online accounts do you have?
  - Banking (e.g., JPMorgan Chase, Bank of America)
  - Cryptocurrency (e.g., Bitcoin, Coinbase)
  - Device Accounts (e.g., Apple ID, Android account)
  - Email (e.g., Gmail, Hotmail)
  - Games (e.g., Steam, Candy Crush)
  - Government Accounts (e.g., IRS, local government services, Medicare)
  - Health (e.g., hospital accounts, insurance)
  - Online Bills (e.g., electricity bill, phone bill)
  - Online Storage (e.g., Dropbox, cloud storage)
  - Shopping (e.g., Amazon, Walmart)
  - Social Media (e.g., Facebook, Whatsapp)
  - Streaming and Entertainment (e.g., Netflix, Spotify)
  - Travel Rewards (e.g., airline rewards, hotel points)
  - Other [text box]
  - None of the above
- Thank you for your interest in this study. Please provide an email where we can reach you if you are selected for the study.
  [text box]

B Interview Script

Before Recording Starts

Hello, thank you for agreeing to participate in our study investigating digital estate planning.

[Interviewers self-introductions]

How would you prefer we address you?

Thanks [form of address]!

Today we're going to talk about steps people may take to make sure others have access to their passwords and anything else needed to access digital accounts after they die or become incapacitated or otherwise unable to manage their own accounts. We will not ask you about the details of your personal holdings or accounts. We are instead interested in how people manage ways to access their digital accounts, such as with passwords, passcodes, or other methods. For the sake of convenience, when we refer to passwords, we mean any of these access methods. Before we begin, I would like to go over some information about this study.

- As previously mentioned, this interview will be addressing potentially sensitive topics such as end of life estate planning and death. If these topics are likely to be distressing to you, you do not have to participate. You may terminate the interview now or at any time.
- When signing up for this study, you consented to participate in this study. [Confirm name, age.]
  - Name: [Full name of participant from the interest survey]
  - Age: [Age of participant from the interest survey]
- Do you have any questions regarding the consent form?
- Do you confirm that you still consent to participate in this study and wish to proceed?
- We will be recording this interview. We will remove your name and other identifiable information if any quotations from this interview are used in published research. Please do not bring up any personally identifiable information during the interview. Do you consent to the video and voice recording?

I will start the recording shortly, do you have any questions or clarifications before we begin?

Alright, I will begin recording. [Start recording]

Intro

I have begun recording. For the record, I will need to capture your consent to participate in this interview.

Consent procedure

- Do you agree to participate in this research?
- Do you agree to the audio and video recording of this interview?

Existing Practices

Thank you! We will start with some general questions about your existing experiences with estate planning and management of digital accounts.

Q: Have you gone through the process of estate planning?

- Prompt (if no specific explanations): inventorying assets in preparation for end of life, writing wills
- Did you discuss digital assets/access to digital accounts during this process?
  - If yes, what was the process?
    - What did you discuss?
    - Who did you discuss with (estate planner, family, both, other)
  - If not, would you have wanted the opportunity to discuss digital account access?

Q: Have you been in the situation where you needed to handle someone else's will or access their online accounts after their death or when they were incapacitated?

- As part of this, did you need access to digital accounts of the deceased [or specific name]?
- If yes, what are some barriers you have encountered in trying to access digital accounts in such cases? (Steer questions to focus on digital accounts)
- If yes, what was useful, what worked? What made it easy to access and why?

Q: What types of online accounts do you use, if any?

- Prompt: Email, social media, banking, utilities, medical
- Do you have any bank accounts you access online? [Note people might just do physical banking]
  - Do you have utility bills you pay online?
  - [Will specifically ask based on the interest survey later]

Q: What do you think/expect will happen to these online accounts after you die or if you became incapacitated and were no longer able to access them yourself?

- Follow-up: give examples of kinds of accounts (email, utilities, banking, social media) or specifically prompt on the accounts mentioned in previous question.
- Do you have processes in place to transfer digital accounts, in the case of death or incapacitation?
  - If yes, ask more specifics.
  - If not, ask why not?
- Prompt participants about keystone accounts (electronic devices) if they do not mention it spontaneously.

Q: (Which categories of accounts do you consider most important to share passwords for…) Passwords to which categories of accounts do you consider most important to share when you die or in case of incapacitation?

- Other examples: Phone passwords/Unlock codes
  - Keystone accounts (email etc.), 2FA
- Follow-up: Why do you consider these accounts important? [Possible prompts below]
  - [Distinguish between access to contents of an account (photos, emails etc.) and being able to use the account (2FA, transfer money, book flights etc.)]
  - Emotional/digital legacy.
  - Important for management of assets.
  - Payment accounts, recurring bills, bank.
- How would you try and share access?
- If don't think any are important (or only one/a few), ask why the rest are not important (maybe don't really use electronic accounts).

Q: Are you aware of any tools for account transfer, password sharing etc.?

- Have you considered planning for account transfer?
  - Why or why not?

Existing/Hypothetical Tools (Password managers, Estate Planner Tools, etc):

Thank you! Now we are going to tell you about a few different options for providing access to digital accounts. Please give us your opinions on these options.

Tool 1: Sharing accounts. [Password sharing, joint accounts, or family accounts.]

Explanation for Tool 1: For example, one fairly simple method of sharing account passwords is pen and paper, or a digital file with account names and passwords. Some people also have existing accounts that are shared between multiple people (e.g., more than one person has the login credentials, people know the password, different accounts can access the same information).

- **Q: Is this a method that you use? [For each, ask participants to clarify if it is a shared password, shared account, or other sharing methods.]**
  [If the participant uses this method, reword the following questions from hypotheticals to present tense.]
- **Q: Who would you give this information to, if you were to use this method? It can be more than one person.**
- **Q: What kinds of accounts would you use this for?**

Tool 2: Legacy Features

Explanation for Tool 2: Some programs provide inactive account managers or legacy contacts, which allow users to determine what happens with information in the account after a certain period of inactivity. For example, Google Inactive Account Manager allows Google Account users to designate a trusted contact to receive a notification and/or specified data (such as emails, photos, or other content) in the Google Account after a designated amount of time the account has been inactive. Apple and Facebook also have similar features.

- **Q: Is this a method that you use?**
  [If the participant uses this method, reword the following questions from hypotheticals to present tense.]
- **Q: Who would you give this information to, if you were to use this method? It can be more than one person.**
- **Q: What kinds of accounts would you use this for?**

Tool 3: Password Managers Explanation for Tool 3: A password manager is a software application that helps you store and manage your passwords for various online services. It essentially acts like a secure digital vault for all your passwords. Examples include:

(1) Password managers built into browsers, such as Chrome, Firefox, etc.
(2) Password managers built into operating systems, such as MacOS Keychain.
(3) Third-party applications installed on devices or browsers, such as 1Password, LastPass.

- **Q: Have you ever heard of password managers (defined above)?**
  - If not, would you be interested in using password managers if they can help you share account access with loved ones/beneficiaries after you pass away?
  - If yes, do you use them to keep track of your passwords?
    - Would you use them for digital asset sharing? Why or why not?
  - What features would you need most in password managers to manage account credential sharing after death?
- **Q: Is this a method that you use?**
  [If the participant uses this method, reword the following questions from hypotheticals to present tense.]
- **Q: Who would you give this information to, if you were to use this method? It can be more than one person.**
- **Q: What kinds of accounts would you use this for?**

Barriers (or advantages)

For each of the three tools – Sharing accounts, Legacy Features, and Password Managers, we ask about each of the following.

Q: [Technical] Barrier: What difficulties do you anticipate in sharing passwords using [this tool], if any?

- Would you prefer pencil and paper/physical methods to transfer data?
- Are there security concerns that arise for you due to the medium of [this tool]?
- Adv: Is there anything about this tool that would make things easier for you?

Q: [Legal] Barrier: Do you think there might be legal barriers in using [this type of tool] to share account information after death?

- Would these legal barriers be a concern for you?
- Adv: Are there legal problems you think [tool] would solve?

Q: [Psychological/Emotional] Barrier: Are there concerns of trust, improper access, account breaches regarding sharing passwords and accounts in case of death and emergency using [tool]?

- [Mention not here to judge password use or practices, just give own thoughts]
- Adv: Anything about this tool that makes you feel good/give reassurance?

Q: [Security] Barrier: Does [tool] raise any security concerns or address some of your security concerns?

- [Give example of security risk such as password being leaked or account being hacked]
- [Prompt for both concerns and advantages if interviewee focus on one or the other]

Q: [Privacy] Barrier: Does [tool] raise any privacy concerns or address some of your privacy concerns?

- [Give example of privacy concern such as leaking of personal/private information, such as personal messages or emails.]
- [Prompt for both concerns and advantages if interviewee focus on one or the other.]

Q: [General]: What are some other questions or concerns you might have about sharing accounts/transferring accounts for access after death or incapacitation using [this tool]?

- Would this tool be helpful for the access credentials you care about?

Conclusion

Q: Given that you've thought more about this type of estate planning and account access, is there anything you might follow up on?

[Discuss study compensation method of $30 with participant.]

Do you have any other questions that you would like to ask us or things you want to mention?

[End Recording]

I have stopped the recording. Thank you again for your participation! Are there any questions or concerns you have that you would like to address off the record?

C Additional Tables

In table 3, we show the number and percentage of participants with each type of online accounts.

Table 3: Self-reported online accounts ownership

Account	Num. Participants	% Participants
Banking	21	100.00
Email	19	90.48
Health	16	76.19
Online Bills	16	76.19
Device Accounts	15	71.43
Government Accounts	15	71.43
Streaming and Entertainment	15	71.43
Online Storage	14	66.67
Travel Rewards	14	66.67
Social Media	13	61.90
Games	5	23.81
Shopping	4	19.05
Cryptocurrency	2	9.52
Other	1	4.76

D Codebook

- **Account**
  - bills
  - device
  - email
  - entertainment
  - financial
  - gaming
  - government
  - medical
  - online storage
  - physical device
  - shopping
  - social media
  - travel
- **Advantage**
  - 2FA
  - automatic
  - backup
  - easy to update
  - keystone account
  - local storage
  - physical security
  - proactive legacy feature
  - security
  - trust in people
  - trust in process
  - usable
- **concern**
  - 2FA
  - data misuse
  - difficult to use
  - digital security
  - disorganized
  - emotional
  - improper use
  - legality
  - location
  - non-pwd identifier

  - none
  - not cross-device
  - not priority
  - number of accounts
  - privacy
  - security
  - security questions
  - technical
  - unable to monitor
  - unclear model
  - updating contact
  - updating passwords
- **consideration**
  - convenience
  - different management
  - ease for others
  - financial info
  - how to share
  - knows it works
  - reputation
  - when to share
- **expectation**
  - close accounts
  - expertise
  - order of operations
- **importance**
  - least
  - most
  - somewhat
- **other**
  - all passwords
  - bureaucracy
  - don't care
  - dual purpose
  - hacked
  - inability to access
  - inactive or unused accounts
  - local copies
  - people help
  - prefer paper
  - redundant
  - resignation
  - scams
  - tech self-confidence
  - unaware of legacy features
  - unaware of tool
  - unclear model
  - want to use tool
- **practice**
  - auto-pay
  - biometrics
  - different roles
  - encryption
  - friend-influence
  - granular control
  - instructions
  - none
  - not formalized
  - not online
  - period check
  - person to help
  - put in legal doc
  - record of accounts and passwords
  - remote app control
  - security and privacy
  - share content
  - skip 2FA
  - stay logged in
  - verify bills
- **reflection**
  - 2FA
  - account order
  - consider
  - deletion
  - discuss with executor
  - include more accounts
  - legacy features
  - legacy features: genology
  - organize things
  - password manager
  - physical security
  - share access
  - travel rewards
  - update records
- **tool**
  - 2FA
  - SSO
  - backup codes
  - digital file
  - inactivity notices
  - legacy feature
  - master password
  - password manager
  - share password
  - shared access
  - shared account
  - tell person
  - won't use
  - writing
- **want**
  - default at setup
  - emergency contact tool
  - granular selection
  - inactivity notices
  - inactivity notices: custom
  - legacy feature
  - legacy feature: 2fa
  - legacy feature: all accounts
  - legacy feature: history
  - memorialize
  - multiple people with access
  - periodic update reminder
  - persistence
  - person to help

  - removal
  - timeliness
- **wills**
  - has will
  - on app
  - online accounts discussed
  - online accounts not discussed
  - planning