The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains

Tal Morse
Hadassah Academic College, Israel

Michael Birnhack
Tel Aviv University, Israel

Abstract
Scholars have observed a gap between users’ stated preferences to protect their privacy and their actual behavior. This is the privacy paradox. This article queries the persistence of the privacy paradox after death. A survey of a representative sample of Israeli Internet users inquired of perceptions, preferences, and actions taken by users regarding their digital remains. The analysis yielded three distinct groups: (1) users interested in preserving privacy posthumously but do not act accordingly; for these users, the privacy paradox persists posthumously; (2) users who match their behavior to their preferences; for these users, the privacy paradox is resolved; and (3) users interested in sharing their personal data posthumously but do not make the appropriate provisions. This scenario is the inverted privacy paradox. This new category has yet to be addressed in the literature. We present some explanations for the persistence of the posthumous privacy paradox and for the inverted privacy paradox.

Keywords
Digital legacy, digital remains, posthumous privacy, privacy paradox

Corresponding author:
Michael Birnhack, Faculty of Law, Tel Aviv University, Tel Aviv 6997801, Israel.
Email: birnhack@tauex.tau.ac.il
Introduction

As our lives go digital, we constantly generate more and more personal data: Online chats and emails; social interactions such as posting, “liking,” and sharing content; comments we write; photos and documents we share; and every other digital activity. After we die, the personal data become digital remains—orphaned data whose creator and owner is now dead. There are continuous political, popular, legal, and scholarly debates about online privacy and the challenges to protect it (Marwick and boyd, 2014). While people express their interest in guarding their privacy, they behave in ways that appear to result in the opposite, such as making their personal data publicly available (Spiekermann et al., 2001). This phenomenon has been termed the privacy paradox (Barnes, 2006; Norberg et al., 2007). Although a better term would be a tension or discrepancy as we elaborate later, we stick to the common term. This article is the first to address the posthumous condition, namely, the persistence of the privacy paradox after death.

In most Western countries, deceased people do not have legal rights regarding their personal data (the European Union (EU) allows member states to regulate personal data of deceased persons, GDPR, 2016, recital 27), but, as we show later, the living often have wishes and preferences regarding the fate of their digital remains. Managing one’s personal data in a dynamic digital environment is difficult in itself, a challenge obviously enhanced in the posthumous condition. Unlike physical possessions—a handwritten diary, photo album, or letters—our digital personal data are stored on servers and managed through online accounts. Unlike physical access to the deceased’s belongings, accessing digital remains often requires the assistance of the online platforms that hold the key to such data. Moreover, digital activity creates meta-data about the identity of the user, location, time, and much more. The collection of meta-data is often hidden from the user in what Pasquale (2015) aptly termed “black box.” Thus, the intermediation of the digital posthumous condition raises numerous new questions about the control of personal data, access to digital remains, and the role of platforms. These are social, technological, and legal questions.

We explore one aspect of this multifaceted picture: Is there a gap between users’ preference regarding their digital remains and their behavior in this regard? In other words, is there a posthumous privacy paradox? As we explain later, our focus is on online social interaction between people; hence, we leave aside the corporate collection and processing of personal data, and we focus on content rather than meta-data, although the latter can contain personal information and indicate content.

We surveyed a representative sample of Israeli Internet users, inquiring of their preferences regarding their digital remains and their behavior in managing access to them. Currently, few options are available for managing one’s own online digital remains: using dedicated tools offered by some platforms (which we discuss later on) or leaving accounts informally accessible to others. We call the latter option informal access: This characterizes the rather mundane situations whereby someone, typically a family member of the deceased, can turn on the electronic device and be logged in to the deceased user’s accounts or use a password list the user created for her own convenience or provided to the family member (e.g. spouse).

The analysis of the survey’s results suggests the presence of a posthumous privacy paradox, which has yet to be discussed in the literature. We identified three different
practices, two of which have been recognized in the literature regarding the in-life privacy paradox. The third practice is novel, unique to the posthumous condition, comprising three user groups. The first group of users is interested in preserving their privacy posthumously and taking their data to the grave but do not make the necessary provisions to fulfill this desire. For this group, the privacy paradox persists in the sense that their behavior does not match their desires regarding posthumous privacy. The second group manages to match behavior to preferences, whether denying access to the digital remains or sharing their personal data posthumously. For this group, the privacy paradox is resolved. The third group is interested in sharing personal data posthumously, but their actions and non-actions are likely to result in the opposite, namely, that the online platforms will block others from accessing the data. We call this latter scenario the inverted privacy paradox, in which users wish to surrender control over their personal data, but the outcome is of imposed privacy. We offer some possible explanations for the persistence of the posthumous privacy paradox and for the inverted privacy paradox.

The next section reviews the literature on the privacy paradox, which has thus far dealt exclusively with living people. We frame the research questions accordingly and present the methodology and findings. A discussion follows. Finally, we suggest further research directions and offer conclusions.

Theoretical framework

The privacy paradox

As the use of the Internet spread in the early 2000s, researchers observed a gap between people’s stated interest in their online privacy and their actual behavior (Spiekermann et al., 2001): While people express an interest in not disclosing personal data, they publish personal information online, accessible to family and friends, online “friends,” platforms, and third parties. This gap—the discrepancy between expressed intentions and actual behavior—was termed the privacy paradox (Barnes, 2006; Norberg et al., 2007).

The privacy paradox matters. In popular and policy debates, both privacy supporters and those who argue privacy is overrated point to either users’ statements or their practices (see Nissenbaum, 2009; Solove, 2020). Indeed, lay observations of users’ widespread publication of personal data online are often referred to as an indication of the abandonment of privacy. However, empirical studies have consistently indicated that perceptions of privacy and users’ interests—millennials included—are to protect their privacy (boyd, 2014; Millham and Atkin, 2018). When the platform enables users to change privacy settings, they often seize this option, especially in the context of social privacy (Schwartz-Chassidim et al., 2020). To anticipate the discussion and state the obvious, the posthumous condition freezes the privacy settings.

The privacy paradox has been found in several contexts, for example, Israeli teenagers (Soffer and Cohen, 2014), Dutch middle adulthood (Van den Broeck et al., 2015), or Australian mothers regarding their children’s privacy (Chalklen and Anderson, 2017; Pangrazio and Selwyn, 2018).

Scholars explored different aspects of the paradox. Norberg et al. (2007) studied the consumer context, finding that the perception of risk affects the declared statements about
privacy preferences. One thread in the literature suggested some nuances. Carey and Burkell (2009) argued that people perceive privacy-related risks in various ways, and these perceptions influence their behaviors. They found that users are more likely to protect privacy in personal relationships than with strangers. Furini and Tamanini (2015) pointed to awareness as an important factor in the assessment of risk and willingness to engage in information disclosure scenarios. Raynes-Goldie (2010) and Young and Quan-Haase (2013) documented various privacy strategies employed by Facebook users especially geared toward other users rather than toward companies. Raynes-Goldie referred to the former as social privacy and to the latter as institutional privacy. These findings suggest that the gap between preferences and practice is contingent upon the perceived recipient of the data. Masur and Scharkow (2016) found that people employ different disclosure management strategies according to the perceived sensitivity of the information they disclose and the perceived audience or recipients. Trepte et al. (2017) pointed to cultural background as explaining differences in privacy perceptions and management.

Another thread in this literature addresses the crux of the paradox, with two main, opposing responses. One response denies the paradox, arguing that people tend to express general concerns regarding their privacy, but once asked to indicate their worries with regard to specific incidents of information disclosure, they tend to be less concerned, and these attitudes coincide with their behavior (Dienlin and Trepte, 2015). Another argument is that in fact, many people make a deliberate choice to trade-off their personal data for some benefit. People might do so either because they are unconcerned of their privacy or because they value a benefit over privacy (Kesan et al., 2016). The paradox may also be explained through privacy cynicism and resignation (Hoffmann et al., 2016). Other studies portrayed privacy negotiations in terms of privacy calculus (Trepte et al., 2017) or disclosure management (Masur and Scharkow, 2016). The latter adds an important finding for our context, which is that “people attribute different levels of privacy to different types of information depending on their individual privacy preferences” (Masur and Scharkow, 2016: 2).

To be able to make such a trade-off decision, people need to know and understand what is at stake (Furini and Tamanini, 2015). Indeed, studies show that users do not read privacy policies (Obar and Oeldorf-Hirsch, 2018) or misunderstand them (Turow et al., 2018), yet studies constantly indicate that people do care about their privacy, even if they do not always know how to protect it. Hence, the “people don’t care” explanation is the least relevant explanation for the privacy paradox (Garga et al., 2014).

The opposite response to the paradox does not deny its existence but, rather, tries to explain the gap between individuals’ expressed interests and their actual behavior, by pointing to various cognitive limitations that determine the preference-behavior gap. Acquisti and Grossklags (2007) conducted several experimental studies suggesting three possible sources of the gap: (1) information deficiency, such as incomplete information or asymmetrical information—namely, that users have insufficient knowledge regarding what happens to their data; (2) bounded rationality—namely, that users replace rational decision-making with simplified mental models and heuristics; and (3) various biases, such as the valence bias, that is, that users overestimate the likelihood of favorable events; the overconfidence bias regarding one’s knowledge and ability; and rational ignorance.

Additional explanations of the paradox include users’ disregard for privacy issues when occupied with subscribing to a new service and perceive such practice as the norm (Obar and Oeldorf-Hirsch, 2018). Hermstruwer (2017: 21) added the temporal
dimension, namely, that “users tend to underestimate the long-term risks associated with the disclosure of personal information.” The latter dimension becomes acute when the long-term risk includes the user’s death.

**The posthumous condition**

Does the privacy paradox persist after death? We use the term “posthumous condition” to refer to the management of dead users’ personal data, namely, their digital remains. Accordingly, the posthumous privacy paradox would be present if there is a gap between living users’ preferences regarding the protection of their digital remains and their actual behavior in this regard. Family and friends of the deceased may be interested in accessing such personal data for purposes of bereavement, memorializing, and commemoration (Bouc et al., 2016; Sofka, 2020). In other words, deceased people’s data may still have value to others, despite their death. However, our focus here is on the data subjects, now deceased, and their ante-mortem wishes regarding their post-mortem privacy, rather than other parties’ needs and interests regarding the deceased’s digital remains.

Users’ preferences regarding the posthumous condition are not formed out of thin air. The availability of offline and online means to control the data is relevant—without such means, preferences are mere desires. Media coverage of cases in which access to digital remains was denied or achieved following a legal or public campaign may also affect preferences, although Sarikakis and Winter (2017) found that people are affected by their own negative privacy experiences, rather than by media coverage of the issues. The law is yet another factor that shapes preferences. In the United States, the United Kingdom, and some other Western jurisdictions (but not all; see Harbinja, 2017; McCallig, 2014), privacy lapses at the person’s death. Exploring whether and how these factors shape preferences requires separate studies. Our purpose here is to decipher users’ preferences regarding their personal, online data in the posthumous condition.

There are few published academic studies of users’ interests or practices regarding the fate of their digital remains (Brubaker and Callison-Burch, 2016; Brubaker et al., 2014), with none conceptualizing the discussion in the framework of the privacy paradox. As noted, understanding the privacy paradox is crucial for optimal policymaking regarding living users, and we add that it is crucial also for the posthumous condition (see Edwards and Harbinja, 2013).

This study was designed to provide an initial understanding of stance about posthumous privacy and behavior concerning the management of digital remains. A provisional analysis of the findings suggests that the privacy paradox, which the literature has heretofore discussed with regard to living people, may also apply to the posthumous condition. To confirm whether this is indeed the case, we compared posthumous privacy preferences and behavior for managing access to digital remains.

Note that privacy preferences and privacy behavior should be evaluated on the background of understanding that individuals are part of social networks (Cohen, 2012). The cited studies found that users care and act more about their social privacy (vis-à-vis other people) than institutional privacy (vis-à-vis corporations). Accordingly, we focus on the former.

The privacy paradox literature has brought forth several explanations, as noted: desirable trade-offs, informational deficiencies, bounded rationality, and cognitive biases. We
need to inquire which of these apply in the posthumous condition: What do users know about posthumous privacy and, specifically, about access to their digital remains; how is their rationality bounded under the specific circumstances; and which biases are at play. There may be further biases; for instance, pondering one’s own death is aversive to most people, and Western society often treats death as taboo. However, once acknowledged, death can cause a change in perceptions or behavior, as the Terror Management Theory (TMT) suggests (Greenberg and Arndt, 2011). Put differently, the very reminders of one’s own mortality can trigger changes to attitudes and a wish to leave behind some kind of legacy. How do these biases affect decisions regarding one’s personal data that would become digital remains?

Research questions

The above discussion informs the research questions.

- **RQ1**: Is there a posthumous privacy paradox?

  This task requires investigating preferences and behavior. Accordingly,

- **RQ2**: To what extent users’ preferences as to the fate of their digital remains vary?

  Two main options are currently available to manage one’s own digital remains. One is *formal access*, by using the online tools offered by some Internet platforms or obtaining access by legal means such as a court order (see e.g., in Germany, Case 183/17, 2018). A second option is to enable, whether intentionally or unintentionally, *informal access* to one’s personal data. This option includes leaving applications logged in so that anyone with physical access to the deceased user’s devices will be able to gain access to the online accounts simply by turning the devices on. Such access can be intentionally facilitated, with the purpose of bypassing the intermediary’s control of the key to the data, or it can be inadvertent and unintentional. Another way of informal access is by leaving a list of passwords in an accessible place. Users might create such a list for themselves, and once dead, others might use it to gain access to the deceased user’s accounts. Accordingly,

  - **RQ3**: To what extent are users familiar with online tools to manage their digital remains?
  - **RQ4**: Of those who are familiar with the online tools, to what extent do they use them? Or, is formal access prevalent?
  - **RQ5**: Is informal access prevalent?

  Once learning about users’ preferences and their actual behavior, we can proceed to juxtapose the two. Accordingly, our ultimate research question finetunes RQ1:

  - **RQ6**: How do people’s preferences regarding access to their online digital remains match their behavior?
Methodology

The current empirical study examined both expressed preferences of people regarding their online digital remains and their report of their actual behavior in this regard. While acknowledging the shortcomings of self-reports (Jensen et al., 2005), we conducted a survey among a representative sample of adult Israeli Internet users in June 2017. A uniform questionnaire was distributed via a computer-assisted web interviewing (CAWI) system to participants of an online panel operated by Shiluv I2R, an Israeli market research company. The survey was completed by 478 respondents. Quotas of gender, ethnicity, age, and geographical location were set in advance and controlled during data collection to ensure a representative sampling of Israeli Internet users. Of the participants, 53% identified as women and 47% as men. Participants’ age ranged from 18 to 70 years, and the average age was 38 ($SD = 14.43$) years. Of the participants, 84% were Jewish, 13% Muslims, and 3% Druze.1

The initial set of questions, presented alongside the findings below, addressed participants’ online practices and activities on three main digital platforms for storing and managing personal data: (1) email accounts; (2) social networking sites (SNS), which are the main sphere explored in the context of the privacy paradox; and (3) online cloud storage services, which often contain personal data. We sought information regarding the frequency of use for these services as well as the nature of activities performed via SNS. These parameters indicate the intensity of use and hence the anticipated scope of the digital remains.

A second set of questions sought to delineate users’ preferences regarding their digital remains. We asked the users about their wishes for each service.

The third set of questions addressed users’ practices. We asked about the online tools offered by Google and Facebook and about informal access.

All the data we present in the tables in the findings section are based on responses to close-ended questions. The questionnaire included few open-ended questions to allow respondents to explain or elaborate. When referring to these, we provide illustrative direct quotations of the respondents.

The data were analyzed using software for descriptive statistical analysis (SPSS) with the purpose of juxtaposing preferences and actual behavior. We obtained the ethical approval for this human subject research from Author B’s Institutional Review Board (IRB). Participants received vouchers for their participation. Measures were taken not to collect identifying data; thus, the authors were prevented from re-identifying participants. All participants provided informed consent and were assured that their answers would not be used for any other purpose.

Findings

Digital remains potential

We first asked participants about their online activities and personal data management: Did they maintain an account on each of the noted platforms? As Table 1 shows, Israeli Internet users use these services regularly and frequently.
The more active the users, the more personal data they generate and, consequently, leave more digital remains. Accordingly, we asked which of the following activities participants performed during the 2 weeks prior to the survey.

Table 2 shows that the most common activities on SNS are of media consumption rather than self-generated content. Uploads of original content are also common, even if less frequent.

From these two tables, we learn that Israeli Internet users are avid users that habitually engage in online activities and produce personal data, which will ultimately comprise their digital remains. The intensity of use indicates the digital remains potential.

**Expressed preferences regarding digital remains**

The first prong of the privacy paradox is the users’ expressed preferences regarding their digital remains: How do users want to manage personal data after their death, in terms of who should have access to the data if at all. While data protection is a rich concept, referring to the management of personal data throughout the data’s lifecycle, here we focus on only one aspect relevant to the posthumous condition, namely, access to the data retained by an online service provider and enabling or preventing access thereto. As noted, we focus on the social domain.

To account for posthumous preferences, we asked about the participants’ general wishes regarding access to their digital remains, per-service.

Table 3 reveals a mixed and complex picture. It demonstrates the variance in users’ wishes as for whether or not they wish to leave full, partial, or no access at all to their
digital remains. Approaches to email, SNS, and cloud services are similar, with 45–50% of users who have accounts on these services indicating that they wish to leave full access to all their digital remains. On the contrary, 31–36% expressed the opposite view, wishing to deny all access to their digital remains. Between them, about a fifth of the participants indicated that they wish to allow access to some content, but not in its entirety. In other words, these users want to scrupulously control access to their digital remains. This finding fits the findings of Masur and Scharkow (2016) that people assess the sensitivity of different types of information about them differently and choose whether, how, and with whom to share personal data. Our findings indicate that the wish to manage privacy in a specific manner, namely, per-kind of information, applies to the posthumous condition. Below, we further elaborate on the identity of the person to have such access.

**Actual posthumous privacy management**

When users die, they can no longer act on their personal data, but in the digital age, some online platforms offer tools for managing personal data posthumously. Thus, the second prong of the posthumous privacy paradox regards the actual behavior of users. The two main options currently available to users to enable or deny other people’s access to their digital remains are using online digital tools and enabling informal access.

Additional means to control digital remains, such as laws regulating who can access which kind of personal data and under which conditions, are currently rare. The United States has pioneered a law that regulates access mostly to estate executors (Uniform Law Commission, 2015). France followed with a law enacted in 2016 (“Loi n°2016-1321”, 2016). In some cases, courts ordered platforms to enable access. For example, a German court ordered Facebook to provide parents access to their deceased daughter’s account (BBC News, 2018). Israel has no such legislation, nor have there been judicial decisions regarding personal digital remains.

**Online tools for managing digital remains.** Google, for all its services, and Facebook, for its social network, offer users online tools to manage their accounts posthumously. These tools offer a solution that focuses on and prioritizes users’ autonomy, allowing them to decide how to handle access to their digital remains.

In 2013, Google launched the *Inactive Account Management*, which enables users to choose what will happen to their various data stored on Google’s servers. They can

| Allow access to all contents | Email (%) | SNS (%) | Cloud (%) |
|-----------------------------|-----------|---------|-----------|
| Allow access to some of the contents | 45        | 45      | 50        |
| Deny access to all contents  | 35        | 36      | 31        |
| n                            | 476       | 434     | 378       |

SNS: social networking sites.

---

**Table 3. Would you like another person to have access to your accounts on the following platforms after you die?**
define whether, after a period of inactivity, the account will be deleted, or whether a
person they choose will be permitted to access a copy of their data. If a user does not use
this tool, subject to a strict procedure, Google can assist family members in terminating
the account or retrieving information from it.

Since 2015, Facebook has offered users the option to determine whether their account
will be deleted after their death or whether they wish to memorialize it and to appoint a
“legacy contact.” Upon receiving notification of a user’s death, Facebook policy calls for
removing the account from the living users’ social space and converts it into a memorial-
ized account (e.g. Remembering John Smith). The legacy contact can order the account
to be shut down or can manage some aspects of it, but cannot access personal corre-
spondence that the deceased might have had with other people.

There is a growing industry of third-party companies that offer various posthumous
control services (Öhman and Floridi, 2018). However, these have yet to achieve popular-
ity in Israel; hence, they were not included in the study.

In the survey, we described these tools and asked participants whether they have heard
about them. Those aware of the tools were asked whether they activated them.

Tables 4 and 5 reveal that awareness of existing tools is low. Only a third of those
aware of these tools have actually activated either of them (6% of the overall sample).2
These findings suggest that formal access to digital remain is not prevalent. The findings
indicate that when it comes to managing end of life, the digital realm is not very different
from the non-digital realm. Similar to medical and financial contexts, people are reluc-
tant to deal with their departure, nor are they zealous to leave detailed instructions for the
day after their passing (Jones, 2016; Yadav et al., 2017). Moreover, our findings indicate
that awareness appears to be an insufficient condition for action, as two-thirds of those
aware of the tools avoided their activation. This is another aspect of the posthumous
privacy paradox, which dissociates awareness and action and complicates the manage-
ment of digital remains.

Having anticipated users’ low awareness and non-use of existing online tools to man-
age digital remains, after introducing these tools, we asked participants whether they

---

**Table 4.** [Description of the tool] Did you hear about this tool? Are you aware of it? \((n = 478)\).

|                  | % of participants |
|------------------|-------------------|
| Yes              | 19                |
| No               | 73                |
| Don’t remember   | 8                 |

**Table 5.** Did you activate the tool?

|                  | % of participants aware of the tool | % of sample |
|------------------|-------------------------------------|-------------|
| Yes              | 32                                  | 6           |
| No               | 61                                  | 11          |
| Don’t remember   | 7                                   | 1           |
| \(n\)            | 86                                  | 478         |
were likely to use them. Participants’ responses indicated their preferences regarding the control and management of their digital remains.

Table 6 suggests that the likelihood of using the existing tools for managing access to digital remains is high. This means that more often than not, users wish to maintain control over access to their personal data, and this wish survives death.

**Informal access.** As noted, users can enable access without resorting to online tools or legal mechanisms, thus enabling their relatives or others de facto posthumous access to their online digital remains. Such informal access is pertinent to the posthumous privacy paradox as it can predict the extent to which orphaned accounts will be accessible upon death. Accordingly, we queried whether someone would be able to access the users’ accounts in their absence.

As Table 7 indicates, in approximately half of the cases, the orphaned accounts will remain accessible upon the users’ death. In most cases, the person intended to have informal access is the user’s spouse.

### The posthumous privacy paradox and the inverted posthumous privacy paradox

Thus far, we have presented data on users’ preferences regarding their digital remains and what they actually do (or not do) to ensure that their preferences are actualized. We
saw that awareness of existing online tools for managing access to digital remains is limited and that actual use is much lower.

We noted one instance of the privacy paradox: Upon learning about the online tools for managing digital remains, most users expressed an intent to use them. Thus, it may be concluded that users wish to control their digital remains (control could mean to enable access, not necessarily to deny it), but do not know how. This situation conforms to one of the paradox’s explanations, namely, information deficiencies (Acquisti and Grossklags, 2007). However, information deficiencies do not tell the entire story, since, as we saw (Table 5), two-thirds of the participants who were aware of the tools did not activate them. Some of them offered explanations such as “I didn’t think about it,” “I haven’t found the time to handle this,” and “I don’t want to think about death.” As these are anecdotal responses, further research is warranted here. We would suggest a psychological bias against dealing with one’s own death.

Due to the respondents’ low familiarity and use of the relevant online tools, we focused primarily on informal access to manage one’s posthumous privacy. To examine the posthumous privacy paradox, we used SPSS to compute two new variables: (1) desire to allow access to digital remains and (2) informal access. These two variables quantify and qualify the phenomenon of the posthumous privacy paradox.

We reorganized users’ preferences regarding sharing or denying access to digital remains on the various platforms. We grouped participants according to three expressed preferences (Table 8): (1) #Share_All: Users indicating their desire to leave full access to their accounts on all three platforms; (2) #Delete_All: Users indicating their desire to deny access to their accounts on all three platforms; and (3) #Mixed: Users wishing to enable partial access to content on at least one platform and users whose answers varied across platforms.

We then reorganized the data regarding users’ actual behavior (Table 9), given that 94% of the sample did not activate the online tools (Table 5). These users were grouped in three categories: (1) users reporting having sole access to all platforms; these users do not enable informal access to their accounts when alive, and upon death, their accounts will not be accessible; (2) users reporting that they keep all their accounts accessible to others when alive, and upon death, their accounts will remain accessible to those who have informal access; and (3) users reporting a mixed approach, enabling informal access to some of their online accounts but not to all; these maintain a specified, per-content approach, and upon their death, some of their data will be accessible, and the remainder locked down.

### Table 8. Aggregated wish to allow access to digital remains in email accounts, SNS, and cloud services.

|                | % of participants |
|----------------|-------------------|
| #Share_All     | 38                |
| #Delete_All    | 27                |
| #Mixed         | 35                |

SNS: social networking sites.
Finally, based on the reassignment of the participants according to their preferences to allow or deny access to their digital remains and the extent to which they currently enable informal access to their accounts, we conducted the following cross tabulation which captures the posthumous privacy paradox:

Table 10 illuminates three possible situations, and one that requires further analysis:

| Preferences                            | Behavior                          | #Delete_All | #Mixed | #Share_All |
|----------------------------------------|-----------------------------------|-------------|--------|------------|
| No informal access to all platforms    | No paradox                        | 0           | -1     | -1         |
| Partial informal access to platforms   | Paradox                           | -1          | Requires further analysis | -1 |
| Full informal access to all platforms  | Paradox                           | -1          | Paradox | 0          |

Table 10. The posthumous privacy paradox matrix (0 denotes “no paradox”; 1 denotes “paradox”; and −1 denotes “inverted paradox”).

No paradox (0)

This category characterizes users (1) who wish to deny access to all their digital remains in all platforms, and indeed, they do not enable informal access; and (2) who wish to allow access to all their digital remains in all platforms and indeed enable full informal access before death. For these users, their requests will be satisfied, thus leaving no paradox.

Posthumous privacy paradox (1)

This category characterizes users (1) who wish to deny access to all their digital remains in all platforms but, in practice, enable partial or full informal access; and (2) who wish to allow access to only some of their digital remains but enable full informal access. These users’ preferences will not be satisfied, and the traditional privacy paradox will persist after death. For this group, we find a posthumous privacy paradox, at least regarding the content to which they desired to deny access.
This is a novel category, yet to be identified in the literature: This category characterizes users (1) who wish to allow full access to all their digital remains in all platforms but, in practice, do not enable informal access across platforms prior to death; and (2) who wish to allow access to only some of their digital remains but enable no informal access before death. These users’ preferences will not be realized, creating an inverted posthumous privacy paradox, according to which access to digital remains will be more constrained than the users’ desire.

Requiring further analysis is the group at the center of Table 10. These are users with mixed preferences regarding the management of digital remains, such as allowing access to only some personal data and, in practice, enable partial access; namely, some people may have informal access to some personal data. A more granular investigation is needed to determine whether the specific preferences and behaviors match. Furthermore, as Table 7 indicates, users may be selective regarding who has access to which type of content, and a more nuanced study is required to discern whether these wishes are fulfilled.

We calculated the distribution of the participants in the sample according to the posthumous privacy paradox typology (see Table 11).

Table 11 reveals the proportion of the various categories of the posthumous privacy paradox: For a majority of users, a paradoxical condition might occur and that the inverted paradox is likely to be the most prevalent.

**Discussion**

Analyzing the juxtaposition of Internet users’ preferences and behavior regarding digital remains provided an account of the prevalence of the posthumous privacy paradox. We found that indeed, this phenomenon exists, but it is nuanced and complex, and it varies among people. A fifth of the sample have no paradox regarding their online digital remains, and their preferences regarding the social domain will be fulfilled after their death. For about a quarter of the sample, given their current responses, the paradox will ensue as we know it; these users’ wish to restrict access to their digital remains will not be fulfilled because of how they currently manage their accounts.

For nearly 40% of the sample, an inverted privacy paradox will occur. These users wish to grant extensive access to their accounts, yet their current practice would indicate that posthumous access will be more limited than they had desired. In other words, the findings indicate that for the vast majority of the sample, an incongruence between
preferences and behavior can be anticipated, and unless users modify their behavior, or unless the platforms or legislatures intervene, their expectations for access to digital remains will be thwarted. We further found that the online tools offered by major platforms are little known and, even more, little used.

Can the explanations offered regarding the privacy paradox for living users explain the posthumous privacy paradox? The factor of insufficient information clearly applies to the posthumous condition. Users do not know enough about how their personal data are processed or how to set the technology in accordance with their wishes. Even for those who are aware, there may be a lack of technological know-how, as to how to manage one’s personal data that would become digital remains. The phenomenon of digital remains is relatively new, and addressing questions of managing digital remains is only emerging. Many users have not attended to what will happen to their online personal data after their death. Furthermore, as the findings show, users are unaware of the possibilities at hand. Thus, even if individuals have preferences regarding their digital remains, they are most likely unaware of the implications of their actions or inaction.

Living users can choose how to handle their personal data, what to disclose, and to whom, and they can change their minds over time. As for the posthumous condition, living users can decide how to manage access to their data posthumously, but, obviously, they cannot change their preferences and instructions after their death. Furthermore, the possibilities for managing access to digital remains are, at present, fairly limited. Thus, posthumous control of digital remains is currently relatively constrained, and the few available options do not necessarily accommodate the diversity of users’ preferences. Other possible explanations of the posthumous privacy paradox are idiosyncratic, stemming from the posthumous condition. We suggest possible biases, which merit further research.

Western culture has complex relations with death. Throughout the last century, death was perceived as a taboo. However, attitudes toward death appear to be changing in recent decades, inter alia, in light of new information technologies (Walter et al., 2012). And yet, it appears that people tend to avoid end-of-life decision-making. This aversion characterizes financial and medical decisions, and as our study shows, this is also the case with personal data. Here, the valence bias (Acquisti and Grossklags, 2007), noted in relation to the privacy paradox, resurfaces in a reconfigured way. As terror management theory (Greenberg and Arndt, 2011) suggests, people do not entertain the possibility that they might die at any moment or at any time soon. Therefore, they avoid making conscious decisions and take actions that would take effect following their death. This attitude can explain why so few have activated the existing tools for managing digital remains. However, as the question of awareness as an explaining factor is also applicable here, further research is needed.

The information deficiencies mentioned above may facilitate the availability heuristic (Carey and Burkell, 2009), which can explain the posthumous privacy paradox. This heuristic points to failures in decision-making due to the lack of relevant information in the decision-makers’ mind. Facebook and Google have only recently addressed the matter and have not made serious efforts to communicate their solutions. In the absence of available information regarding the phenomenon or about people that have dealt with the consequences of access or denial of access to digital remains, users are less likely to process information about it in a way that will motivate them to act. Another explanation
from the original privacy paradox—risk management—can be considered (Norberg et al., 2007). Since users are uninformed about the possible unfortunate scenarios of their actions or inaction, and since they have not experienced it first-handedly, they lack a perception of the risks involved, thus stymying their taking appropriate measures (see Sarikakis and Winter, 2017).

Our analysis points to the phenomenon we termed inverted posthumous privacy paradox. Here, the mismatch between preferences and behavior is that others cannot access the user’s digital remains, despite the latter’s pre-death desire. Such access could have facilitated others’ efforts to memorialize the user, but under the inverted privacy paradox, this desire is left unfulfilled. Can the explanations offered in the literature regarding the privacy paradox explain the inverted situation? As this case deals with a wish to bestow others with access to one’s personal data, explanations of limiting access become futile. However, the explanation denoting information deficiency and valence bias may apply here, as people are unaware of possible dire consequences of their inaction and downplay negative scenarios. To this, we add individuals’ low awareness of the online tools, namely, Legacy Contact and Inactive Account Manager (IAM), and a reluctance to deal with one’s own death. These potential explanations require further study.

Finally, the findings can inform policymaking. Privacy rights in Common Law jurisdictions expire when the person dies. In the digital environment, intermediaries store the data and hold the keys to it. Thus, when a person dies, family and friends of the deceased require the assistance of the service providers to gain access to the data. Dealing with these intermediaries makes things more complex legally, and the few cases that have reached courts were decided with mixed outcomes. Some jurisdictions, namely the United States and France, have attempted to regulate access to digital remains. Indeed, if policymakers could identify a broad consensus on the matter, they could assist in fulfilling users’ preferences. However, our findings indicate that people have different preferences regarding access to their digital remains, thus rendering a unified policy unsuitable. Another legislative option could be to set default rules, such as enabling full access to digital remains or, conversely, denying all access, accompanied by an option to change the default. Again, our findings indicate that at present, the information deficiencies and various biases against managing afterlife would mean that most users would not change the pre-set default, and based on previous research, they are less likely to do so as they grow older (Van den Broeck et al., 2015).

Further research

The posthumous privacy paradox merits further research. We point to some potential avenues.

First, supplementary qualitative research can shed light on the preferences for managing digital remains and the reasons that may explain the gap between preferences and actual behavior. Theories in social psychology, namely, TMT, seek to explain individuals’ decision-making in light of impending death. These theories have yet to be applied to digital remains.

Second, a comparative study may assist in identifying the factors that are most relevant to the management of digital remains. While death is socially and culturally contingent,
and attitudes toward death change over time and space, the global information technology (IT) corporations currently deploy a uniform policy. Thus, there is a tension between global policies and local norms. Where the issue is regulated, local law adds further complexity.

**Conclusion**

Online privacy is much debated nowadays. The amorphous nature of privacy, the fast-changing technologies, and commercial and political pressures (see Zuboff, 2019) pull in different directions, resulting in a dramatic, yet unresolved, battle. One of the features of this flux is the privacy paradox: the gap between people’s preferences regarding their privacy and their actual behavior, especially in the social realm. This article adds yet another aspect to this debate—the posthumous condition, namely, when self-generated personal data become digital remains upon the death of the person. This becomes a pressing issue as more people leave digital data behind, and the number of digital users who die continues to rise. This study sought to theorize and empirically account for the phenomenon we identified as the posthumous privacy paradox.

Based on a quantitative survey of Israeli Internet users, we documented the gap between stated preferences and actual behavior and found that the privacy paradox is likely to apply in the posthumous condition. Indeed, some users manage to fit their behavior to their preferences, whether intending to prevent access to their digital remains or to share it upon their death with people they choose. However, the majority of users are interested in fulfilling their preferences posthumously, and for them, the privacy paradox will persist after death. The findings indicate that the posthumous privacy paradox applies in two situations. One is a mismatch between privacy-oriented preferences and an opposite behavior, and another, yet undiscussed in the literature, is the inverted mismatch, characterizing users who wish to share their personal data posthumously with their loved ones, but that given the current policies of major online service providers, the absence of a legal framework, and their own uninformed inaction, these wishes are likely to be frustrated. This is the inverted privacy paradox.

We believe that user studies can inform policy, as the current study exemplifies. The findings indicate that a top-down, one-size-fits-all law will frustrate the wishes of large segments of the user population. Given the low awareness to the management of personal data and to the currently available technological tools, and the inhibiting factors at play regarding death, default rules, whether initiated by the platforms or by legislation, are likely to stick. Our study calls for better ways to increase user autonomy so that each person can decide for himself or herself the fate of their digital remains.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Israeli Internet Society (ISOC-IL) (no grant number) and Israel Science Foundation (ISF) (Grant No. 257/18).

**ORCID iD**

Tal Morse [https://orcid.org/0000-0002-9960-620X](https://orcid.org/0000-0002-9960-620X)
Data availability statement

The data set is open and freely available on the website of the Israeli Internet Society (in Hebrew), at http://bit.ly/digital-memories-isoc-excel

Notes

1. In 2016, women were 51% of the Israeli population; Muslims were 17%, and Druze about 2% (https://www.cbs.gov.il/EN/pages/default.aspx).
2. Facebook refused to provide us with data about the actual use of its tool.
3. Replying to open-ended questions (“Why did you choose not to activate the online tools for managing digital remains?”).
4. Facebook occasionally changes its policy regarding the manner in which it receives a notice about a user’s death and might memorialize the profile without assigning a legacy contact.

References

Acquisti A and Grossklags J (2007) What can behavioral economics teach us about privacy? In: Gritzalis S, Lambrinoudakis C, di Vimercati S, et al (eds) Digital Privacy: Theory, Technologies, and Practices, New York: CRC Press, pp. 363–377.

Barnes SB (2006) A privacy paradox: social networking in the United States. First Monday. Epub ahead of print 4 September. DOI: 10.5210/fm.v11i9.1394

BBC News (2018) Facebook ruling: German court grants parents rights to dead daughter’s account, 12 July. Available at: https://www.bbc.com/news/world-europe-44804599

Bouc A, Han S-H and Pennington N (2016) “Why are they commenting on his page?” Using Facebook profile pages to continue connections with the deceased. Computers in Human Behavior 62: 635–643. DOI: 10.1016/j.chb.2016.04.027

boyd d (2014) It’s Complicated: The Social Lives of Networked Teens. New Haven, CT: Yale University Press.

Brubaker JR and Callison-Burch V (2016) Legacy contact: designing and implementing post-mortem stewardship at Facebook. In: Proceedings of the 2016 CHI conference on human factors in computing systems, New York, pp. 2908–2919. ACM. Available at: https://research.fb.com/wp-content/uploads/2016/11/legacy-contact-designing-and-implementing-stewardship-at-facebook.pdf

Brubaker JR, Dombrowski LS, Gilbert AM, et al. (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, New York, pp. 4157–4166. ACM. Available at: https://cmci.colorado.edu/ldlab/assets/bibliography/pdf/Brubaker2014a.pdf

Carey R and Burkell J (2009) A heuristics approach to understanding privacy-protecting behaviors in digital social environments. In: Kerr I, Lucock C and Steeves V (eds) Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society. 1st ed. Oxford; New York: Oxford University Press, pp. 65–82.

Case ZR III 183/17 (2018) Available at: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=86602&pos=0&anz=1

Chalklen C and Anderson H (2017) Mothering on Facebook: exploring the privacy/openness paradox. Social Media + Society 3(2): 2056305117707187.

Cohen JE (2012) Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven, CT: Yale University Press.

Dienlin T and Trepte S (2015) Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology 45(3): 285–297.
Edwards L and Harbinja E (2013) Protecting post-mortem privacy: reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment* 32(1): 83–129.

Furini M and Tamanini V (2015) Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications* 74(21): 9795–9825.

Garga V, Bentobn K and Camp LJ (2014) The privacy paradox: a Facebook case study. In: *TPRC 41*, Arlington, VA. Available at: https://www.coursehero.com/file/21790551/SSRN-id2411672/

GDPR (2016) Regulation (EU) 2016/679 of the European parliament and of the council. Available at: http://data.europa.eu/eli/reg/2016/679/oj/eng

Greenberg J and Arndt J (2011) Terror management theory. In: Lange PAMV, Kruglanski AW and Higgins ET (eds) *Handbook of Theories of Social Psychology: Volume One*. Los Angeles, CA: SAGE Publications Ltd, pp. 398–415.

Harbinja E (2017) Post-mortem privacy 2.0: theory, law, and technology. *International Review of Law, Computers* 31(1): 26–42.

Hermstruwer Y (2017) Contracting around privacy: the (behavioral) law and economics of consent and big data. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 8: 9.

Hoffmann CP, Lutz C and Ranzini G (2016) Privacy cynicism: a new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(4): Article 7.

Jensen C, Potts C and Jensen C (2005) Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63(1–2): 203–227.

Jones JM (2016) Majority in US do not have a will. Available at: http://news.gallup.com/poll/191651/majority-not.aspx

Kesan JP, Hayes CM and Bashir MN (2016) A comprehensive empirical study of data privacy, trust, and consumer autonomy. *Indiana Law Journal* 91(2): 267–352.

Loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, § art. 63 (2016). [in French].

Marwick AE and boyd d (2014) Networked privacy: how teenagers negotiate context in social media. *New Media & Society* 16(7): 1051–1067.

Masur PK and Scharkow M (2016) Disclosure management on social network sites: individual privacy perceptions and user-directed privacy strategies. *Social Media + Society* 2(1): 2056305116634368.

McCallig D (2014) Facebook after death: an evolving policy in a social network. *International Journal of Law and Information Technology* 22(2): 107–140.

Millham MH and Atkin D (2018) Managing the virtual boundaries: online social networks, disclosure, and privacy behaviors. *New Media & Society* 20(1): 50–67.

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Norberg PA, Horne DR and Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41(1): 100–126.

Obar JA and Oeldorf-Hirsch A (2018) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23(1): 128–147.

Öhman C and Floridi L (2018) An ethical framework for the digital afterlife industry. *Nature Human Behavior* 2: 318–320.

Pangrazio L and Selwyn N (2018) “It’s not like it’s life or death or whatever”: young people’s understandings of social media data. *Social Media + Society* 4: 1–9.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
Raynes-Goldie K (2010) Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. First Monday 15(1). Available at: https://firstmonday.org/ojs/index.php/fm/article/view/2775

Sarikakis K and Winter L (2017) Social media users’ legal consciousness about privacy. Social Media + Society. Epub ahead of print 1 February. DOI: 10.1177/2056305117695325.

Schwartz-Chassidim H, Ayalon O, Mendel T, et al. (2020) Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy. Heliyon 6(2): e03298.

Soffer T and Cohen A (2014) Privacy perception of adolescents in a digital world. Bulletin of Science, Technology & Society 34(5–6): 145–158.

Sofka C (2020) The transition from life to the digital afterlife: thanatechnology and its impact on grief. In: Savin-Baden M and Mason-Robbie V (eds) Digital Afterlife: Death Matters in a Digital Age. Boca Raton, FL: Routledge, pp. 57–74.

Solove DJ (2020) The myth of the privacy paradox. George Washington Law Review 89. GWU Legal Studies Research Paper No. 2020-10. Available at: https://papers.ssrn.com/abstract=3536265

Spiekermann S, Grossklags J and Berendt B (2001) E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM conference on electronic commerce, pp. 38–47. Available at: http://ec-wu.at/spiekermann/publications/inproceedings/E-privacy%20in%202nd%20Generation%20E-Commerce.pdf

Trepte S, Reinecke L, Ellison NB, et al. (2017) A cross-cultural perspective on the privacy calculus. Social Media + Society 3: 205630511668803.

Turow J, Hennessy M and Draper N (2018) Persistent misperceptions: Americans’ misplaced confidence in privacy policies, 2003–2015. Journal of Broadcasting & Electronic Media 62(3): 461–478.

Uniform Law Commission (2015) Fiduciary access to digital assets act. Available at: https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=61b22f86-6d3f-fd1f-735b-5e113f866c60&forceDialog=0

Van den Broeck E, Poels K and Walrave M (2015) Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. Social Media + Society. Epub ahead of print 5 July. DOI: 10.1177/2056305115616149.

Walter T, Hourizi R, Moncur W, et al. (2012) Does the Internet change how we die and mourn? Overview and analysis. OMEGA—Journal of Death and Dying 64(4): 275–302.

Yadav KN, Gabler NB, Cooney E, et al. (2017) Approximately one in three US adults completes any type of advance directive for end-of-life care. Health Affairs 36(7): 1244–1251.

Young AL and Quan-Haase A (2013) Privacy protection strategies on Facebook: the Internet privacy paradox revisited. Information, Communication & Society 16(4): 479–500.

Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 1st ed. New York: PublicAffairs.

Author biographies

Tal Morse is an adjunct lecturer at Hadassah Academic College in Jerusalem. His research focuses on media and death, especially death online and mediated death rituals. His book, The Mourning News: Reporting Violent Death in a Global Age was published by Peter Lang (New York) in 2017.

Michael Birnhack is associate dean (Research) at the Faculty of Law, Tel Aviv University. His research focuses on information law, especially privacy and intellectual property. His 2010 book, Private Space (in Hebrew), won the Political Scientists Association Annual Prize.