What happens to my online social estate when I am gone? An integrated approach to posthumous online data management

Leila Bahri, Barbara Carminati, and Elena Ferrari

STRICT Social Lab, Insubria University, Italy

***Abstract*—Technology and the digital world have been making an important part of people's lives nowadays. As death is unquestionably a crucial and fundamental part of life, technology and the digital world ought to play an equally important role in end of life issues as well. For instance, the adoption of online social networks (OSNs) has been amplifying to cover large numbers of the world's population playing big roles in shaping their daily life, in documenting their life experiences, and in sharing their moments with their friends in the network. While current systems focus on the provision of usable and attractive features of their OSN services, considerations of the faith of the online accounts, identities, and data created and shared in their realms when the owner is mo more available to manage them have not been equally taken. In this paper, we raise and discuss issues related to the design and to the provision of integrated services for a posthumous data management that would respect the wills of users all while being concealed to their survivors. We survey the existing practices, we discuss their limitations, and we suggest an integrated approach to posthumous data management based on posthumous data planning assisted by data categorization and automated tools.**

***Index Terms*—Post-mortem online social data, online social networks, online social estate, social digital legacy, posthumous digital data planning.**

I. Introduction

Mechanisms in support of controlled information sharing in the realms of the social web represent one of the main building blocks and of the critical factors to the long term success of any online social networking service (OSNs). This comes also with number of challenges especially related to the design and to the enforcement of technical solutions that support fine-grained access needs, that offer privacy preservation guarantees, that provide assistance and awareness tools, and that are verifiable and usable within the implementing system. The traditional view to this problem mostly assumes that the desired functionality is known; that is, the privacy requirements are clear, and based on them it is understood how the data has to be treated [1]. The challenge to solving the problem is then primarily resumed in ensuring that this actually happens. However, this traditional view to access control and privacy management collapses when the user (i.e., data owner) becomes suddenly not available to manage her/his data.

In fact, the explosion of OSNs adoption and their growing maturity has introduced a new challenge related to the management of data usage and unexpected access scenarios of post-mortem online activity. Based on some recent research reports [2], in 2015 there are about 4353 million email accounts open, and about 4078 million active social networking accounts with about 1319 million users manipulating them. With a world annual death rate of about 8 deaths per 1000 population [3], rough estimates can be made as of the number of dead people who held ownership of at least one OSN or an email account. For instance, according to a report by *The Huffington post* [4], 20 million accounts on Facebook in 2012 belonged to dead people. According to [1] it can be roughly estimated that 9300 users of Gmail die per day. This suggests that there should be a substantial number of instances and of requests to OSN providers for dealing with *digital estate*. The challenges to answer such instances are more complicated as current users, mostly, do not consider the formulation of *posthumous digital data planning* that could contain guidelines to data usage and access control of their posthumous digital social data [5]. Moreover, current OSNs are still lagging behind in providing platforms that allow for the formulation or that assist in the creation of such posthumous digital data planning [1]. However, real cases demonstrate problematic instances wherein the bereaved faced serious issues related to dealing with the digital data and the online social activity of their lost ones. Indeed, number of true stories exemplify situations in which the bereaved did not know how to deal with this data, needed to get access to it but failed to, or wished to suspend it but were faced with terms of use and legal obstacles [6]. This suggests that one of the critical services to address this problem might be to offer support for *posthumous digital data planning*, based on which users data can be managed respecting their privacy needs/wills even when they are no more available to do it.

Like data access and privacy preferences largely differ from user to another, based on personal preferences, on cultural backgrounds, and/or on the type of data in question, the formulation of such posthumous digital data planning would also considerably vary depending on the circumstances in which it is to take effect, on the types of data it covers, and on the personal preferences of the subject user. For example, a user who runs an OSN page to advertise for some social activity or for an NGO might want his page to be inherited and not frozen or suspended. On the other hand, an artist, for instance, who uses her OSN account to advertise for her pieces of work might require keeping posthumous ownership of her works and possibly designate a person to manage it within some specified guidelines. Clearly, many users might need to plan for their social networking data quite differently. Moreover, users might have different criteria based on which such plans are to be executed in terms of timing and behavior. Therefore, the provision of a platform for users to plan for the management of their data when they are no more available to take care of it requires answering number of integrated and intermingled technical challenges and should not be limited to simple data ownership transfer.

The goal of this paper is to discuss this issue of posthumous data management and to lay the ground for the design of a service package that would allow OSNs users to make their digital data planning with assisting tools. Basically, we suggest that such planning should be performed with respect to different data types and to corresponding actions and management styles to be attributed to them. Moreover, we pinpoint and discuss the technical challenges related to the automated and integrated execution of these plans. Clearly, one of the challenges is also in designing solutions to better detect when such plans can take effect and that will be resilient to attacks that might exploit them to gain illegitimate access to protected content.

The remaining of this paper is organized as follows: in Section II we survey and discuss currently available approaches to post-mortem data management either in research works or as deployed in major OSN providers. In Section III we provide an overview of our suggested integrated approach based on data categorization and we discuss the related technical requirements, challenges, and opportunities; whereas, in Section IV we present further discussions on other possible scenarios. We conclude the paper in Section V and we outline future works.

II. Currently available approaches to the management of posthumous data

There are number of online sites and a considerable amount of digital material that involves issues related to death, bereavement, and grieving. However, technological tools in this sensitive area are still not well developed to answer the requirements emerging from a need to manage the online legacy of users after they have passed away and offering support to their grieving families and friends [7]. When it comes to online social networking services and sites, additional challenges appear in considering social digital legacy management and the needs of the bereaved. On one hand, there is the challenge of preserving users privacy and security preferences even after they have gone. On the other hand, there are the needs of the deceased user's families and friends [8], [9]. Moreover, there is the issue of whether all this generated content is to be simply thrown to nonexistence, or it might hold precious contributions to the intellectual or social realms and that would need to be commemorated, saved, or memorialized. In this section, we provide a brief review on current practices and approaches to the management of online social data of the deceased, and we discuss the limitations that they represent.

A. Current features in social networking services

It is not until after they have been running for some considerable time that current major OSNs and email providers have started to think about ways to deal with accounts and data of the dead. At the beginning, accounts would be automatically deactivated or expire after some time of inactivity measured by the duration since the last login to the account was performed [ref]. With the massive growth in the adoption of online services that require the creation and management of online identities and of online accounts, and with the explosion in online content generation, people's online lives have been becoming of substantial relevance to their existence. Hence, these online lives have also required proper management after the real life of their owners end. As a response to emerging problems and scenarios that required management of the online accounts of the deceased beyond deletion or expiry, some systems have made trials to answer this yet challenging and new requirement to the provision of their services.

For instance, Google has introduced in 2013 a feature called the *Inactive Account Manager* [10]. Google users can select up to 10 trusted contacts from their contacts list to entrust them with their data, or selected portions of it, should they become unable to manage and use their accounts (mostly because of long inactivity that would refer to death). Users can set the length of their inactivity period beyond which Google will execute their pre-prepared plan regarding their chosen trusted contacts and the specified data that they would like to transfer to them. Basically, users can choose to have their data deleted or sent to some of their chosen trusted contacts. Google hopes that this initiative would help its users to plan their digital afterlife in alignment with their security and privacy choices and also in a way that would make the task easier for their loved ones. This feature being better than having the account with all its related data simply expire still suffers from some limitations. For instance, users can choose to have their data, or selected portions of it, sent to their nominated trusted contacts; however, they cannot put any restriction on what could be done with this data or on how it could be utilized. That is, the data ownership is intuitively transferred to the trusted user who receives it. For instance, if a Google user has generated number of videos and published them on Youtube, once access and control over these videos is passed to their trusted contacts they become their owners. This might violate intellectual property rights.

On the other hand, accounts of the deceased on Facebook used to get frozen and to change in type to a *memorial account* [11]. A Facebook memorial account would still be available to its friends based on the privacy preferences set by the account owner when the account was still active, but will not be available in public searches deleting by this the possibility of receiving new friends requests. Moreover, login to a memorial account is disabled and no access to its private messages or to any of its non shared content with friends is permitted. However, the user's friends can still interact on the account and live/express their grief through it. Very recently (early in 2015), and as a response to the cases in which family or friends of the deceased needed to export some of their lost ones' data, Facebook updated its policy regarding this issue and started offering three options from which users can select while still alive [12]. In particular, they can choose to: 1) have the account completely deleted, 2) have the account become a memorial page of their life and experiences, or 3) users can choose to allow an identified person to manage their account after they have gone. This nominated account manager will not have access to all the account (private messages are still inaccessible, for example), but he/she will be able to download an archive of the account's photos, information, and posts, he/she will be able to publish a post that would appear at the top of the memorialized page, and also to change the profile and the cover pictures. This feature also suffers from the same limitations as the inactive account manager by Google. Moreover, given the nature of the information generated and shared on online social networks, such as Facebook, this feature of nominating a manager for the account of a deceased brings up new limitations. For example, users can create and manage pages on Facebook to advertise for some ideas, to organize business, etc. Such pages would need to have a different faith, after the passing away of their creators, than deletion, that will cause their valuable contributions to get permanently lost, or proper inheritance that would fully transfer ownership. Moreover, users might have some valuable content in their private messages that they would have liked to donate or to share with someone. For example, a user who has suffered from depression and who has documented her state of minds in some private exchange with a doctor or with a trusted person might want to have all this data reused for some research or medical purposes given they are anonymized, for example. Clearly, planning for post-mortem management of online social data requires techniques that support more fine-grained options and rules beyond simple inheritance or deletion of content.

B. Third party tools for posthumous data management

There are number of emerging online tools that provide services and features to users to help them plan for the management of their online data after they have gone. Most of these focus on providing some online support to the families and friends of the deceased by having some automated pre-saved messages sent to them after the death of the user is confirmed/communicated to the system.[1] Another innovative service called Perpetu[2] provides its users with the possibility of formulating an online legacy specifying their wishes regarding the management of their online accounts after their death. Users can choose to have the system add one last post to their Facebook timeline, for example, have their emails automatically transferred to some named person(s), delete their content on some given network, or set their contributions to some coding communities (such as GitHub) to open-source, among others. Perpetu not only offers a platform for the formulation of a user's digital legacy but offers its enforcement as well. Perpetu claims that it does not require access to users accounts; however, privacy related issues, possible attacks to exploit the system for malicious access, and other security related issues are yet to be investigated and studied. Moreover, systems such as perpetu present third party services that not all users of online social networks and sites might be knowledgeable about; hence, hindering their adoption. This also suggests that there are promising fields of research related to the study of such third-party services and their implications especially in terms of the privacy and safety of their users.

C. Inheritance vs. stewardship for social digital legacies

One of the works in the literature that tried to look into this issue of data inheritance and of social digital legacy is presented in [13]. According to the authors, inheritance calls for ownership transfer whilst digital legacies represent more than collections of digital assets. That is, digital legacies might represent identities, social interactions, intellectual properties, and other activities that identify the user. Moreover, inheritance requires the definition of a heir, thing which mostly does not apply to online accounts and online social data that mostly represent users identities and are not simple transferable property. Therefore, the authors suggest the concept of stewardship as an alternative to inheritance when dealing with the management of post-mortem online social data. The authors have come to their suggestion based on a series of qualitative interviews that they have conducted with subjects who have witnessed at least one contact with a Facebook account of a deceased friend. Basically, the authors highlight the fact that OSNSs accounts represent more than a collection of data that can be inherited or represented in an archived memorial. In fact, these accounts are also part of social interactions that might continue even after the account owner has died. This has been witnessed to be the case through memorial practices of the deceased's survivors. As such, the authors suggest to build a system that offers a platform for the continuation of such posthumous online social activity within circles and groups that respect the initial connections that have been established by the deceased. They suggest that those people will act as stewards or mediators who extend the online activity of the deceased without owning their accounts or their identities or their data.

Putting it up all together, we can see that the management of post-mortem online data is still in its emerging states. We can also notice that the different approaches and techniques already available for this purpose can be applicable to some types of data and in some contexts, but have serious limitations in others. For this, we suggest in the following section an integrated approach that bases on merging all of these techniques and apply each of them based on the type of data in hand and the given context. We also discuss the technical challenges that result from such intended integration.

[1] Examples of these services are: www.ifidie.net, www.afternote.com, etc

[2] www.perpetu.co

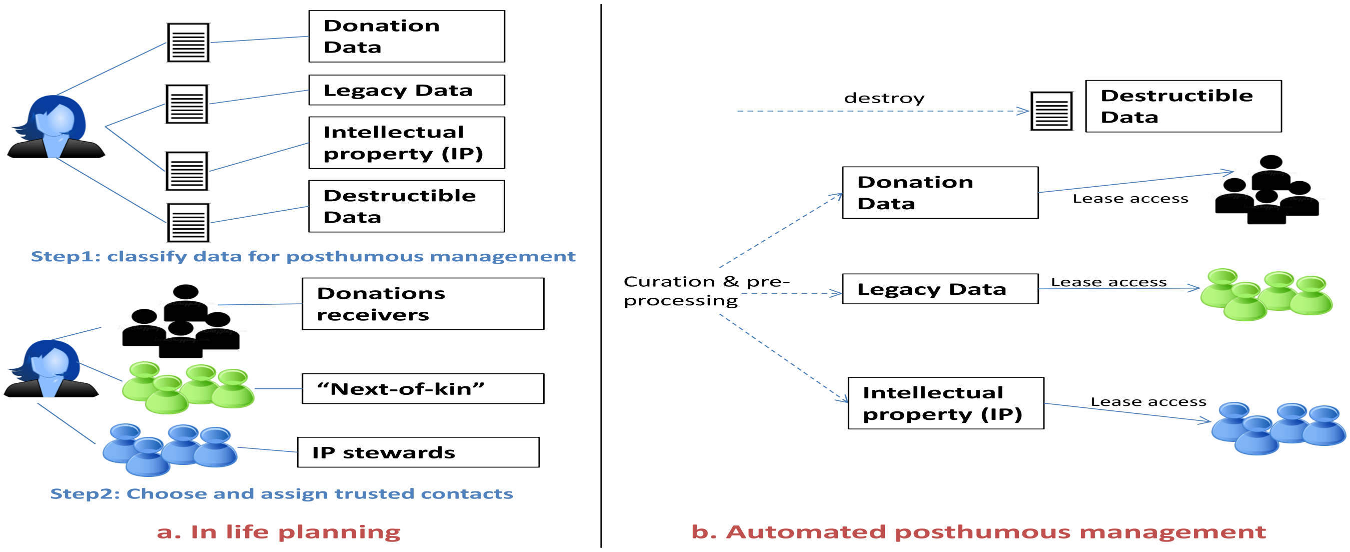
Donation Data
Legacy Data
Intellectual property (IP)
Destructible Data
Step1: classify data for posthumous management
Donations receivers
"Next-of-kin"
IP stewards
Step2: Choose and assign trusted contacts
a. In life planning
destroy
Destructible Data
Donation Data
Lease access
Curation & pre-processing
Legacy Data
Lease access
Intellectual property (IP)
Lease access
b. Automated posthumous management

Fig. 1: Overview of the suggested integrated approach to digital data planning and posthumous data management

III. An Integrated Approach to Posthumous Management of Online Social Data

Considering the different types of data generated and owned by OSNs account holders, we suggest a framework that combines different approaches to posthumous data management based on an integrated logical view of user data. Our suggested framework, as depicted on Figure 1, is made of two main phases: 1) supporting and assisting users for posthumous social digital data planning while they are alive, and 2) executing the plan after their death is confirmed. We assume that the framework is supported by the OSN provider(s) with whom the user has online social accounts. That is, we assume that the OSN implements the framework or allows for its concealed and secure interfacing to get access to and to manage all users' data held in users accounts. In addition to this, we also underline the importance of having a usable solution that provides users with easy-to-understand and easy-to-configure interfaces. Clearly, the issue of planning for posthumous data management should not be a pleasant task in itself, and as such usability of the offered system should get even a higher importance.

The first phase of the framework concerns the provision of an assisting platform for users to prepare posthumous digital data planning for their online social data. We propose basing this planning on categorizing social data into four main categories that reflect the major post-mortem data management needs as extracted from an integrated analysis of available related suggestions ([1], [13]), and of high level discussion articles on the topic [14], [15]. As depicted on Figure 1.a, we propose assisting users to categorize their social data as: *donation data*, *legacy data*, *intellectual property*, or *destructible data*. We explain these suggested categories as follows:

- Donation data: this would make any pieces of information that the user would like to contribute with to the advancement of science or of research. For example, a user might wish to have her digital traces regarding her shopping habits to be donated to some research group or organization that might value the availability of such data to the advancement of their findings. The suggestion of this category comes from the idea of allowing to users similar management styles of their real and tangible estate in the realms of the social digital world as well. Indeed, number of people wish to have some of their property, or all of it, donated for charity or for research [16], [17] and this is one of the available and quite common forms for the management of estate [17]. Similarly, and given the value that the online social data might hold for the development of science and of research in different domains, we believe that a holistic framework for posthumous social digital data management should support this type of wills as well.
- Legacy data: by this we refer to the data that the user would like to have inherited by some of their friends or family members. Legacy data should not be referring to or making part of a user's identity as identities are fundamentally not inheritable. Photo albums, music playlists, e-books collections that can be legally transferable,[3] or some published content for which the user does not want to hold intellectual property are examples of types of data that could go under this category.
- Intellectual property: as the name suggests, this would refer to any created data that the user thinks has an intellectual value and of which they would like to keep posthumous ownership. Examples of data that could make an intellectual property are photos taken by professional

[3] Copyrights on some e-books might prohibit their legal sharing with others [18]; however, this remains as an open question on whether these copyrights apply to the management of posthumous property as well or not.

photographers, drawings, created videos, created music, etc.

- Destructible data: this refers to any data that the user would like to have automatically deleted without letting anyone get hold of it. This can cover any type of data depending on the personal preferences of the user. Some users, for instance, might choose to have all their accounts with all their content destructible.

After categorizing their data, users would have the possibility of selecting people or entities to whom they would like to entrust the different categories of data they have and the levels of privileges they would like to transfer to them. As on Figure 1.a: step 2, users choose the entities that would receive their donation data, stewards for the management of their intellectual property data, and people who would inherit their legacy data (i.e., next-of-kin). We note here that while next-of-kin is normally defined by law regarding the transfer of estate, we consider in this model that users explicitly choose and define their next-of-kin. That is, the inheritors in our framework might be people who are not related to the next-of-kin defined by law. We suggest this as digital legacies from OSN data does not constitute tangible property or is not, thus far, under the types of estate typically managed by laws. Moreover, we also note that users can select different people or entities to entrust with each of these posthumous data categories. For instance, a user should be able to specify different types of donation data and link each of it to a different receiving entity, such as precising that shopping records should go to a research group X and health related records should go to a medical entity Y. Likewise, users can also specify different stewards for different types of their intellectual property data (e.g., music should be moderated by friend Bob and poems by friend Kate), and different inheritors for their legacy data based on specified access rules.

The second phase of the framework consists at making the plan take affect after the death of the account owner is confirmed. Upon such confirmation, that we discuss later on, the system automatically deletes all the destructible data (possibly sending a deletion confirmation message to a designated survivor if such confirmation is desired and specified by the deceased in the plan), and leases access to the designated entities based on the settings pre-prepared by the deceased account owner (see Figure 1.b).

We further detail each of these two phases and discuss the related challenges and technical issues and opportunities in what follows.

A. Digital data planning for posthumous management

As presented earlier, the first phase of our suggested framework consists at having users prepare a digital data plan for their online social data posthumous management. This planning concerns the categorization of data and the designation of people, and/or entities, to entrust with it. We believe that planning for posthumous social digital data management based on the categorization suggested in this paper would help users better understand the types of management available to their data based on its importance and on its meaningfulness to them. However, assisting tools should also be provided to support users in making their categorization decisions. The research community in the domain of data labeling [19], [20], patterns learning [21], topics modeling and detection [22], [23], content popularity prediction [24], recommendations of settings based on similarity with better informed users [25], etc., provides works that could be re-utilized to help users and assist them to better plan or express their posthumous data management wills. For instance, techniques related to topics modeling (see for example [23], [22]) might be used to make recommendations and suggestions to users regarding the data that could make their intellectual property or the one that could better fit or help as donation data. Similarly, the system can be trained to predict the user's preferences regarding the distribution of their legacy data and how they would like it to be inherited. For example, similar to privacy settings in active accounts, users can specify inheritance rules for their legacy data specifying that content that is related to work goes to their colleagues or to some of them, holiday photos go to their partners, music play-lists go to their siblings, etc. The system can assist with this by making suggestions, possibly relying on the homophily principle and inferring from decisions already taken by their friends as is already explored and suggested for privacy settings recommendations, for instance (e.g., see [25]).

Similarly to assisting users with the categorization of their data, another requirement for the system would be to provide users with needed information that would allow them to better choose their designated posthumous data managers. For instance, a user Jane might choose her colleague Kate to receive an archive of all her work related posts forgetting the ones that she has not preliminary authorized her to view or in which she complained about her or negatively commented about her behavior. In here, text analysis and sensitive content identification, as also anticipated in [1], might provide users with the needed elements and information to better make their choices. Moreover, the system can also suggest and enforce rules related to the privacy preferences set by users for their active accounts. For example, the system might enforce that the posts archive that would be transferred to Kate from Jane's account would contain only those posts that Kate was allowed to view when Jane's account was still active.

B. Posthumous digital data plans execution

When it comes to plans execution, two main challenges can be foreseen. The first one is related to the timing of execution. That is, the system would need a mechanism by which it can learn that the account owner has passed away and it is time to put the posthumous digital data plan into execution. The second challenge relates to the curation and to the processing of data in a concealed way that respects the wills mentioned in the plan and that leases access to designated entities in alignment with the plan's rules.

1) Execution timing: There are not many ways for the system to learn of the passing away of a user. Typically, this could happen either by detecting an inactivity long enough to deduce that the user is no more alive, given the inactivity period technique is used. Or, survivors of the deceased user would inform the service provider submitting necessary documentation. The first option of setting an inactivity period might represent two problems. First, it is tricky to set the length of an inactivity period upon which it is to be understood that the user has passed away. Indeed, setting short periods, of couple of months for instance, might seem to some frequent heavy users of the OSN as the right period to set; however, new situations might emerge in their life making them unable to use their OSN account though they are still alive. For instance, users might be detained, unexpectedly hospitalized, etc., and hence they would not like the posthumous plan to get into execution but might neither have the means to declare it to the system. On the other hand, setting a long period might come with the inconvenience of delaying the execution of the plan and might result in managerial problems for the survivors of the deceased.

The second option of having the survivors of the deceased inform the service provider also comes with limitations. The survivors, for instance, might not choose to report the event so that they could still interact with the account. This might go against the will of the deceased who had developed plans and who wished to have them executed upon their death. Besides, there might bureaucracy procedures and documentation complications (related to translations, verification, authentication, etc.) that might slow down the process or even make it unfeasible. This might be the case especially when the service provider operates in a country that has limited interaction with the country of the deceased user. Such a scenario would make considerable number of instances.

Our suggestion with this execution timing challenge is to adopt a hybrid approach that combines the inactivity period with some automated techniques based on behavior change detection or on the mining and analysis of interactions on the target account. For instance, friends of a deceased might continue to interact with her account demonstrating through it grieving practices similar to those known for funerals [13]. Text mining techniques and automatic tools for observing activity change might be deployed for the system to understand the change of status of the accounts of deceased users. This can be combined with a double-checking procedure by sending confirmation messages to the account of the deceased and to the friends that they used to interact with the most, for instance.

2) Data curation and processing: Once the timing of the plan execution is confirmed, the system needs to put the plan into effect. First, the system needs to locate all destructible data and have it automatically destroyed. Second, the system should notify the designated data receiving entities and lease to them access to the data that was left for them by the wills of the deceased account holder. Before leasing such access, the system needs to support automatic tools for concealed curation of the data so as to not reveal it in forms that would hinder the wills of the deceased related to their privacy settings and preferences. We discuss this curation process by data category in what follows:

- *Donations data*: donations data would need to be processed and to be made in a format that does not identify the donator. For example, this data would need to be anonymized by removing all sensitive content referring to persons proper names or to identifying entities such as locations or institutions. This can be achieved by exploiting techniques for text mining [21], sensitive content detection by topic modeling [23], [22], for instance, or automatic data labeling [20], [26], [19]. Moreover, the system should support automatic concealed communication channels of this data to the designated entities by the deceased in the plan. For example, the system might have the data automatically emailed to a designated research group.
- *Intellectual property data*: intellectual property data would require proper management and curation to ensure its copy rights and to lease it to its designated managers in a form that would protect it against misuse or falsification. The literature offers number of techniques for the protection of intellectual property based on different forms of secure digital signatures (see for example [27], [28]). Such solutions could be considered for adaptation to deal with and to secure this category of posthumous social intellectual property data.
- *Legacy data*: for legacy data, the system needs to ensure the enforcement of the inheritance rules specified in the plan in an integrated way and across all the social accounts covered by the plan. Moreover, the system should support the formatting of this data and its presentation, regardless of its source, in a form of receivable collections that would be passed to the inheritors in a concealed way that respects the privacy wills of the deceased.

In addition to those challenges related to the timing of the plan execution and to data curation, there also comes the challenge of securing the plan against possible abuse and/or attacks that might exploit it to gain illegitimate access to content, either during the user's life or after her death. Moreover, there is also the issue of taking the plan to satisfactory execution when the designated stewards, managers, and/or inheritors of the deceased users are also not available. This is a predictable scenario as there are cases where families or groups of friends all die together like in natural disasters or unexpected incidents such as road accidents, fires, etc. For tangible property and the estate managed by law, this goes down following a next-of-kin line. Could this also be a possibility for the social digital estate? And if yes, what would be the policies and the rules that would define such chains of successors. Moreover, what are the guarantees of the system and how can it (the system or the service provider) provide evidence that the posthumous management of the deceased social data has been carried out in due alignment with the plan they have left, and to whom such evidence should be presented? Such questions remain open for further study and research and are also crucial to the success of any honest trial to manage post-mortem online social data.

IV. Further scenarios and extended discussions

All the discussions presented thus far concern systems that are centrally managed and that have a known service provider. However, the issue of posthumous data management becomes even more challenging and more complicated considering peer to peer and decentralized socializing systems. While many privacy advocates believe that decentralized architectures for the provision of social networking services might be the answer to the privacy preservation problem [29], the development and support of some services such as the management of post-mortem data might represent real challenges to such systems. That said, fertile fields for research and innovation in this domain are available and still weakly addressed or explored.

In addition to this, it would also be equally important to analyze and to study the challenges related to a seamless and integrated management of online social data across different service providers. That is, the design of a common system or protocol that would be spoken by all the available online social networking providers allowing by this one single point of configuration and planning for users to address their posthumous data management issues all at once. Such an integration could, for instance, concern the development of a common standard for the specification and formulation of posthumous data plans all while leaving the proper enforcement locally at the hands of each service provider depending on its deployed technologies. This would be beneficial to users in terms of usability and interoperability, but its conception and design would first require the elaboration of and agreement on common standards and laws regarding the management of post-mortem issues by the different major players of online social networking in the market nowadays. This also calls to the need for high level standards and regularization from the responsible entities regarding this issue of post-mortem management of online social estate.

V. Conclusion and Future Work

We have discussed and raised issues related to the management of posthumous online social data. We have argued that different tactics and management styles should be integrated to offer a system that supports and answers the different requirements of the different types of data generated and owned in the realms of online social networks. We have also surveyed the current practices in deployed OSNs and the few related research works and we claim that there is still much to be done, both from the research body and from OSN providers, to provide tools and services that allow for concealed and satisfactory management of online social estates.

We believe that the research community has yet a lot to do regarding services and systems in support of post-mortem online data management. Given the young age of online social systems, this issue might not seem so pressing now; however, this also remains one of the crucial elements to consider for a long term success and a healthy continuity of these systems.

As future work, we plan to investigate these issues more closely starting with field studies via interviewing and prototype sketching to better understand the needs and the expectations of current OSN users. We also plan to design and develop a system that would integrate the suggested elements in this paper based on categorizations of data and on the exploitation of assisting and automated tools.

Acknowledgment

This work is partially supported by the iSocial EU Marie Curie ITN project (FP7-PEOPLE-2012-ITN).

References

[1] S. Micklitz, M. Ortlieb, and J. Staddon, “”i hereby leave my email to...”: Data usage control and the digital estate,” in *Security and Privacy Workshops (SPW), 2013 IEEE*. IEEE, 2013, pp. 42–44.

[2] T. R. Group, “Email Statistics Report, 2013-2017,” 2013. [Online]. Available: http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

[3] E. G. Network, “World Birth and Death Rates,” 2011. [Online]. Available: http://www.ecology.com/birth-death-rates/

[4] J. Kaleem, “Death On Facebook Now Common As ’Dead Profiles’ Create Vast Virtual Cemetery,” 2012. [Online]. Available: http://www.huffingtonpost.com/2012/12/07/death-facebook-dead-profilesn2245397.html

[5] M. Zhang, C. Jennett, M. Malheiros, and M. Sasse, “”data after death: User requirements and design challenges for snss and email providers,” in *Memento Mori: Technology Design for the End of Life (CHI Workshop 2012)*. UCL, 2012.

[6] G. A. FOWLER, “Life and Death Online: Who Controls a Digital Legacy?” 2013. [Online]. Available: http://www.wsj.com/articles/SB1000142412 7887324677204578188220364231346

[7] M. Massimi and R. M. Baecker, “Dealing with death in design: developing systems for the bereaved,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 1001–1010.

[8] K. E. Graves, “Social networking sites and grief: An exploratory investigation of potential benefits,” Ph.D. dissertation, Indiana University of Pennsylvania, 2009.

[9] C. Maciel and V. C. Pereira, “The internet generation and its representations of death: considerations for posthumous interaction projects,” in *Proceedings of the 11th Brazilian Symposium on Human Factors in Computing Systems*. Brazilian Computer Society, 2012, pp. 85–94.

[10] A. Tuerk, “Google public policy: Plan your digital afterlife with Inactive Account Manager,” 2013. [Online]. Available: http://googlepublicpolicy.blogspot.it/2013/04/plan-your-digital-afterlife-with.html

[11] M. Moore, “Facebook introduces ’memorial’ pages to prevent alerts about dead members,” 2009. [Online]. Available: http://www.telegraph.co.uk/technology/facebook/6445152/Facebook-introduces-memorial-pages-to-prevent-alerts-about-dead-members.html

[12] A. Tuerk, “Heres What Happens to Your Facebook Account After You Die: New policy allows one last post after your death,” 2015. [Online]. Available: http://time.com/3706807/facebook-death-legacy/

[13] J. R. Brubaker, L. S. Dombrowski, A. M. Gilbert, N. Kusumakaulika, and G. R. Hayes, “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*. ACM, 2014, pp. 4157–4166.

[14] J. P. Hopkins, “Afterlife in the cloud: Managing a digital estate,” *5 Hastings and Science Technology Law Journal*, vol. 210, 2013.

[15] J. P. Hopkins and I. A. Lipin, “Viable solutions to the digital estate planning dilemma,” *Iowa Law Review Bulletin*, vol. 99, p. 61, 2014.

[16] C. Castillo, “Donation As An Estate Planning Tool (A Discussion on Donors Tax),” 2014. [Online]. Available: http://www.foreclosurephilippines.com/donation-estate-planning-donors-tax/

[17] B. Schiffman, “Donation Motivation,” 2003. [Online]. Available: http://www.forbes.com/2003/02/21/cx_bs_0221home.html

[18] H. Schmundt, "The Digital Paradox: How Copyright Laws Keep E-Books Locked Up," 2014. [Online]. Available: http://www.spiegel.de/international/zeitgeist/how-copyright-laws-prevent-easy-sharing-of-e-books-a-961333.html

[19] R. Mihalcea, "Unsupervised large-vocabulary word sense disambiguation with graph-based algorithms for sequence data labeling," in *Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 2005, pp. 411–418.

[20] R. Yan, J. Yang, and A. Hauptmann, "Automatically labeling video data using multi-class active learning," in *Computer Vision, 2003. Proceedings. Ninth IEEE International Conference on*. IEEE, 2003, pp. 516–523.

[21] M. W. Berry and M. Castellanos, "Survey of text mining," *Computing Reviews*, vol. 45, no. 9, p. 548, 2004.

[22] J. Zeng, J. Duan, W. Cao, and C. Wu, "Topics modeling based on selective zipf distribution," *Expert Systems with Applications*, vol. 39, no. 7, pp. 6541–6546, 2012.

[23] L. AlSumait, D. Barbará, and C. Domeniconi, "On-line lda: Adaptive topic models for mining text streams with applications to topic detection and tracking," in *Data Mining, 2008. ICDM'08. Eighth IEEE International Conference on*. IEEE, 2008, pp. 3–12.

[24] G. Szabo and B. A. Huberman, "Predicting the popularity of online content," *Communications of the ACM*, vol. 53, no. 8, pp. 80–88, 2010.

[25] A. Srivastava and G. Geethakumari, "A privacy settings recommender system for online social networks," in *Recent Advances and Innovations in Engineering (ICRAIE), 2014*. IEEE, 2014, pp. 1–6.

[26] M. Khodabandeh, A. Vahdat, G.-T. Zhou, H. Hajimirsadeghi, M. J. Roshtkhari, G. Mori, and S. Se, "Discovering human interactions in videos with limited data labeling," *arXiv preprint arXiv:1502.03851*, 2015.

[27] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Watermarking techniques for intellectual property protection," in *Proceedings of the 35th annual Design Automation Conference*. ACM, 1998, pp. 776–781.

[28] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "Fpga fingerprinting techniques for protecting intellectual property," in *Custom Integrated Circuits Conference, 1998. Proceedings of the IEEE 1998*. IEEE, 1998, pp. 299–302.

[29] L. A. Cutillo, R. Molva, and T. Strufe, "Privacy preserving social networking through decentralization," in *Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on*. IEEE, 2009, pp. 145–152.