

PASSING AND PASSING ON IN THE DIGITAL WORLD – ISSUES AND SOLUTIONS FOR THE DIGITAL ESTATE

Elke Brucker-Kley *, Thomas Keller *, Kurt Pärli **, Claudia Pedron *,
Matthias Schweizer **, Melanie Studer **, Pia Wohland***

*Zurich University of Applied Sciences, School of Management and Law, Winterthur, Switzerland,
<http://www.sml.zhaw.ch/en>,*

**Department General Management, Institute of Business Information Management, **Department
Business Law, Center for Social Law, *** Newcastle University, Institute for Ageing and Health,
Newcastle upon Tyne, U.K.*

ABSTRACT

What happens to the large volume of information on social media and other Internet platforms after our death? Even while alive it is extremely difficult for anyone to control the storage and dissemination of personal data on the Internet. How and why should we therefore try to make arrangements regarding what happens to this data when we pass away? Our next of kin do not usually know much about our various online activities, nor do they have access to the passwords necessary to deactivate profiles and delete or move information. At the same time, platform providers follow different practices, and their terms and conditions vary considerably. This paper summarizes the results of an interdisciplinary research project¹ aimed at clarifying the many open questions there are in connection with this topic and proposes an extended perspective on how the many facets of this subject might be approached.

KEYWORDS

Digital Estate Planning, Digital Inheritance, Digital Legacy, Social Media, Mortality Rates, Right to Be Forgotten

¹ Co-financed by the Commission for Technology and Innovation CTI, Innovation Promotion Agency (Swiss Federal Department of Economic Affairs)

1. INTRODUCTION: FROM DATA STORAGE TO DATA GRAVEYARD

It may be considered slightly morbid to calculate the mortality rates of social network users, especially if this is done in the context of digital estate planning, a relatively new field of business. Drawing on this, Nathan Lustig, one of the founders of Entrusted², a company offering digital estate planning services, has calculated that 1.5 million Facebook users died worldwide in 2010 (Lustig, 2010, 2012). His calculation is based on age-group mortality rates in the US, which he applied to Facebook user statistics. The results of this numbers game were reflected in the impressive headline: “Three Facebook Users Die Every Minute“, thus positioning the concept of “digital death” in countless blogs and articles, and increasing the awareness that social media users are neither forever young, nor are they immortal. Applying Lustig’s approach to Facebook’s member base in Switzerland results in a mortality rate of roughly 1 per 1,000 members for 2011 (Table 1). As the results for 2012 indicate, this mortality rate will inevitably rise, since, on the one hand, the member base ages naturally and, on the other hand, the 50+ age group, although still relatively small, has the highest growth rate in social networks generally (Brucker-Kley e.a., 2013, SocialMediaSchweiz.ch, 2012).

Table 1. Mortality rate of Social Network users (Example: Facebook Switzerland)

Age group	2011 Facebook Switzerland				2012 Facebook Switzerland			
	Mortality rate per 1000 inhabitants ¹	Average active users 2011 (Jan-Dec) ³	Deaths of active users (calculated)	Overall mortality per 1000 active users	Mortality rate per 1000 inhabitants ¹	Active user 2012 (May) ³	Deaths of active users (calculated)	Overall mortality per 1000 active users
14-19	0.2	528'870	95		0.2	531'940	106	
20-29	0.4	858'070	311		0.3	890'020	279	
30-39	0.5	568'920	286		0.5	625'840	293	
40-49	1.3	349'320	440		1.2	417'080	483	
50-59	3.1	163'280	498		3.2	212'180	669	
60-64	6.3	40'150	253		6.4	54'500	350	
>64 ²	12.3	60'590	744		12.2	102'400	1'248	
Totals		2'569'200	2'627	1.02		2'833'960	3'430	1.21

¹Mortality rates for 2011 and 2012 were calculated using population and deaths data available from the Swiss Federal Statistical Office (BFS-1,-2)

²For the age group >64 the mortality rate for people between 65 and 74 was used in both years;

Mortality rate for the age group >64 would be 38.3 in 2011 and 38.8 in 2012

³Source: Facebook statistics edited by (SocialMediaSchweiz.ch)

It is impossible to ascertain how many of these profiles have remained unchanged or how many have been transferred to “memorial” status since Facebook does not remove inactive profiles. It can therefore only be assumed that an unquantifiable portion of all profiles of deceased members continues to “exist”, not only in membership statistics and search results, but also in the form of automatically-generated birthday reminders, networking recommendations, etc. Facebook is only one of many platforms through which, large amounts of data are amassed over the course of a user’s lifetime. This paper sheds light on the main issues related to a digital estate and evaluates approaches to digital estate management.

² Entrusted (Madison, WI) was acquired by Swiss online data safe provider SecureSafe (DSwiss AG) in April 2011.

2. THE DIGITAL ESTATE: ITS RELEVANCE AND PROBLEMATIC NATURE

How can we untangle an online life that has been focused on connecting, sharing, and weaving a highly distributed web? The main issue in dealing with a digital estate is not only its actual **content**; what is equally important are the **platforms** – increasingly Internet-based – where this content is stored and shared with others, the **accounts** to which it is linked, which include personal profile data, and, finally, the **traces** we leave behind, which can be analyzed, as we move through the Internet. What are these digital assets and traces that are accumulated on the Internet over the course of a lifetime? Are they actual assets or do they have emotional value? Are they “digital belongings”, aspects of a “digital identity” - or mere “garbage data”? It is difficult to describe the content of a typical digital estate or make statements about its scope or relevance since the range of possibilities is so extensive: from data storage in the Cloud, to social media profiles, to avatars which store personal characteristics such as voice, appearance, or preferences. The contents may be everything or nothing, valuable or meaningless, intimate or confidential, under copyright or actually illegal. The individual behavior patterns of the various Internet generations and individual users are too distinctive; the Internet business models are too dynamic, permanently introducing new offers and opening up new possibilities for accumulating, disseminating, and evaluating data. As opposed to physical documents, folders, address books, or photo albums, digital assets are, by definition, intangible. During a user’s lifetime this is a normal feature of the increasing digitalization and virtualization of our daily lives. When a user dies, however, this immateriality presents problems which make it complicated for the next of kin to deal with the digital estate of a deceased family member:

- **Knowledge**

Increasingly, an individual’s digital estate is not stored locally on their end devices but is dispersed over various Internet platforms. The deceased person’s dependents usually have no knowledge of these Internet accounts or social media activities. An Internet reputation management service can be useful in tracking down this information but it may not necessarily find everything, particularly if the deceased user had taken full advantage of the available privacy options. In addition, the digital identity of the deceased may not correspond with their actual identity if they had adopted different online personas (avatars, nicknames, aliases, etc.). Whether these “digital identities” should continue to exist without the knowledge of the deceased person’s next of kin is not only a question of piety, but it can also have serious financial consequences, for instance when a contract with a commercial website hosting provider is automatically renewed, or when a Paypal account has an open balance.

- **Access**

Unless the deceased person had deposited access information for online accounts, their dependents will have no easy way of accessing this data and will therefore have to rely on the practices and the general terms and conditions of the platform providers. There are only a few Internet services which have explicit guidelines for dealing with data and accounts in the event of a user’s death (Chapter 4). Some Internet services will grant access to family members who submit a death certificate, regardless of the deceased account owner’s privacy rights. Others have very strict rules which prohibit access by third parties even in the event of a user’s death (e.g., Yahoo! Terms of service (Yahoo!, 2012) expressly state: “*No Right of Survivorship and Non-Transferability. You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death.*”).

- **Ownership and Control**

The issues of access and ownership are closely linked. Sole usership of Internet content is in most cases waived by the users themselves – be it by accepting the provider’s general terms and conditions or by sharing data with other users. When the user dies, it is almost impossible for heirs or other surviving dependents to (re-)gain control over the digital estate, assert their claim to the deceased person’s data, or succeed in having the data deleted (Avok, 2012).

- **Data Worth Preserving and Its Format**

Dying is closely linked to memory. How and by what would I like to be remembered? What might I leave behind that could tarnish people’s memories of me? If important things such as photos, family recipes, or correspondence only exist in digital form, it makes sense to preserve at least part of this “digital estate” for posterity and make it accessible long-term.

- **Erasability and “Digital Forgetting”**

Even while a user is still alive, it is almost impossible to wipe out all traces of their Internet use. Technological advances such as the indexing and analysis of Internet content, multisite postings, or exchange formats make it easier for users to search for and share information. At the same time, these advances also make it harder to enforce the “Right to Be Forgotten” on the Internet. A picture or a profile can be deleted from a platform, but it will continue to exist in the cache of the Internet search engines and web archives; erasing these widespread traces takes effort and persistence.

3. SCENARIOS FOR THE DIGITAL ESTATE

Do our online lives continue when we pass away? Not necessarily. What happens to Internet accounts, profiles, and data in general after a person’s death largely depends on the actors concerned and the four factors outlined in table 2.

Table 2. Actors and factors influencing the destiny of the digital estate

Actors	Factors
Myself Self-determined user	1. Is there a digital estate plan? <ul style="list-style-type: none"> ▪ By what means (conventional will, digital estate planning service, sharing access data with next of kin/trusted friends?) ▪ How should the respective accounts, profiles, and data be treated: deleted, preserved, memorialized, last message, etc.?
Surviving dependents, trusted friends	2. Do/Should my family and/or friends have access to my digital estate after my death? <ul style="list-style-type: none"> ▪ Do/Should they know about my various Internet accounts, profiles, and online data? ▪ Do they have enough Internet or social media know-how to carry out my wishes? ▪ Do my wishes match those of my next of kin and/or friends? ▪ Are my wishes/the wishes of my family and/or friends enforceable against platform providers?
Platform providers	3. How do platform providers treat the accounts and data of deceased users? <ul style="list-style-type: none"> ▪ What terms of use/terms and conditions or other regulations apply? ▪ How do these regulate the transferability of access rights, data, or user rights of living or deceased users? ▪ Where is the company registered, where is its customer service located, and what is the place of jurisdiction? ▪ What documents must be furnished (and in which language) as evidence of the user's death (death certificate, certificate of inheritance, etc.)?
Legislation, jurisdiction	4. What legal provisions apply specifically to digital estate planning and the execution of a deceased person's will? <ul style="list-style-type: none"> ▪ What is the legal status of the content of a digital estate? Is it relevant in terms of succession law, copyright law, or contract law, or is it covered by an individual's personal rights? ▪ How can I dispose of my digital estate in a manner that is legally enforceable? ▪ How can data protection regulations be enforced, e.g., to force a provider to delete data or to deny next of kin access to a deceased user's data? ▪ What are the possibilities and barriers with regard to the enforceability of the wishes of the deceased and their next of kin? ▪ What country has jurisdiction and what is the applicable law in the case of a dispute?

Figure 1 provides an overview of the scenarios which can arise as a result of the fundamental decision for or against digital estate planning.

The outcomes of the two scenarios clearly show:

- **Various ways already exist for Internet users to dispose of their digital estate in a self-determined and proactive manner** (Chapter 5).
- **Internet users who dispose of their digital estate create transparency and prevent access problems from arising for their dependents after they pass away.** Digital estate planning places the control and the power of disposition mainly in the hands of the dependents, who can use the deposited access details to carry out the last will of their deceased relative.
- **If Internet users do not dispose of their digital estate while they are still alive, the platform providers will dictate what happens to it when they pass away.** The different practices of platform providers are discussed in the next chapter.

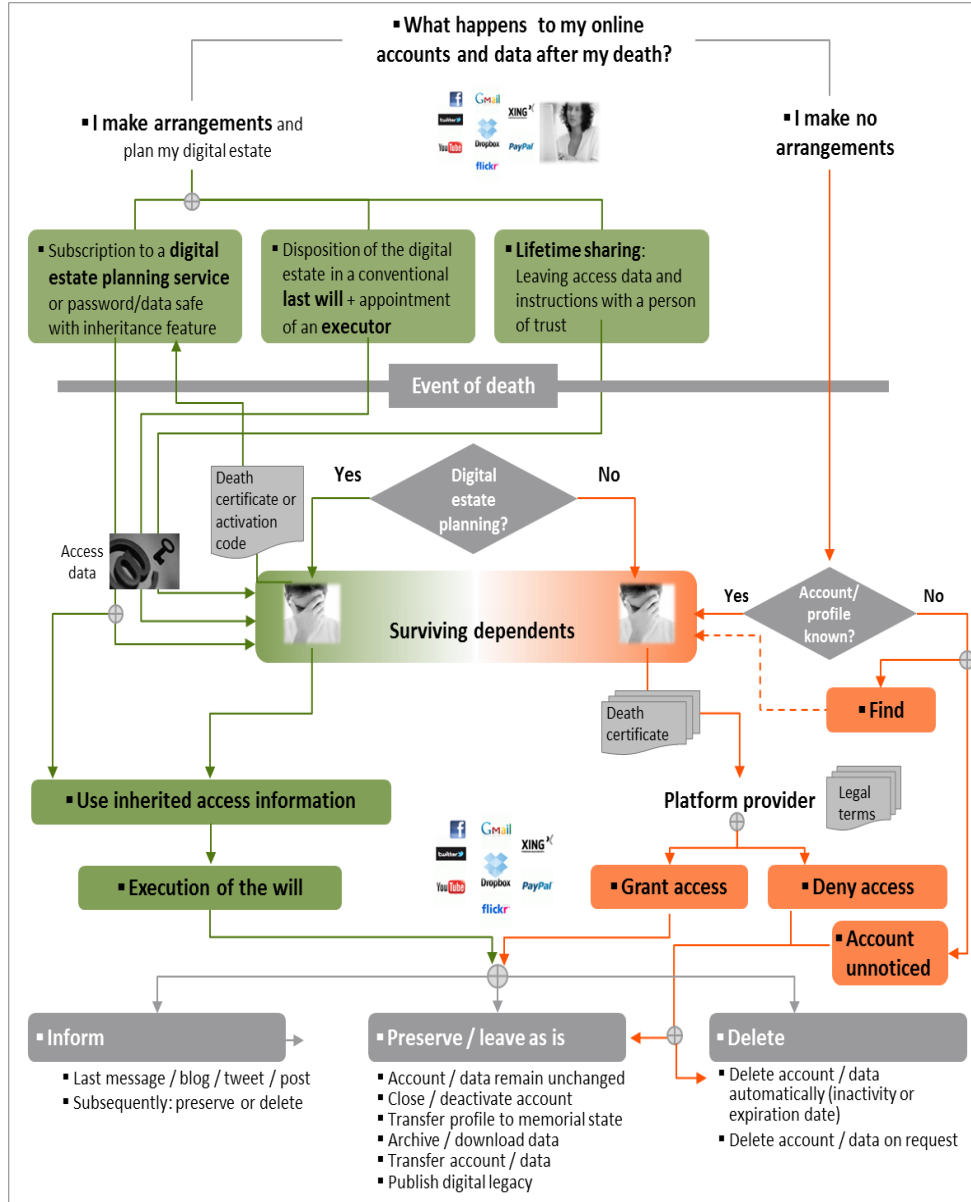


Figure 1. Scenarios for digital estate planning and execution of a will

4. PRACTICES OF ONLINE PLATFORM PROVIDERS

It is mainly the major international online platforms which have regulations relating to a user’s death, usually communicated through the terms of use or the online help feature. Some national or regional providers have regulations which are available from customer services.











	Options during lifetime or with inherited access info			Options enabled by platform providers in the case of a deceased user						+ possible - not possible (+) potentially possible
	Close / deactivate account (profile & data remain undeleted)	Delete account and data	Download data (synchronize, archive)	Dependents may request:						
				Provider deletes inactive accounts automatically	Access to the account	Closure / deactivation of the account	Removal of the account (delete profile and data)	Copies of data	Memorial status	
	+	+	+	-	-	-	+	-	+	Current practice for handling the case of a deceased account holder Option 1: Memorialize profile (Facebook, n.d.) Facebook transfers profiles of deceased members to memorial status. A deceased member can be reported by family or friends (+obituary). Once memorialized, only confirmed friends can find, view, and post on the deceased persons profile. The profile no longer appears as a suggestion. Option 2: Delete profile (Facebook, n.d.) Verified immediate family members can request the removal of the profile (+birth and death certificate of the deceased, proof of identity and kinship).
	+	+	+	-	-	+	+	-	-	No published practice: Network contacts or dependents may report a deceased member to the Xing customer service (no death certificate or other proof required). Profiles of deceased users are closed (i.e. turned inactive) and deleted after 3 months in order to avoid deletions based on a fake call or a mistaken identity.
   	-	+	+	(+) Inactive Account Manager	(+) Inactive Account Manager	-	(+) Inactive Account Manager	(+) in rare cases	-	Practice published in the Gmail help (Google, 2012): Google may provide access to the Gmail content (not the account) «in rare cases» to an «authorized representative of the deceased user». Dependents have to start a two-stage process. In stage 1, the authorized representative has to furnish a notarized death certificate in English, proof of identity, and a copy of an e-mail conversation with the deceased to Google Support (Mountain View, CA). Stage 2 may require an order from a U.S. court and/or submitting additional materials. Since 2013 Google offers an "Inactive Account Manager" that allows users to tell Google what to do with a Google account after a period of inactivity defined by the user (Google, 2013). Users can tell Google to delete the account and all related content in Google services (Gmail, Youtube, Picasa etc.) OR leave up to 10 trusted persons who are granted access once the account is inactive and the user does not respond to a Google alert.
 	-	+	+	(+) after 4 months	-	-	+	-	-	Practice according to the Yahoo! Terms of Service (Yahoo!, 2012) : « Accounts are non-transferable and any rights to Yahoo! ID or contents terminate upon the users death ». Free accounts and expired Pro accounts may be deleted after 4 months of inactivity based on the Yahoo! Terms of Service. However Flickr states in their support forum that they currently do not delete inactive accounts after 4 months. Dependents can request the removal of a Flickr account (+death certificate).
	+	+	-	+	-	+	+	-	-	Practice published in the Twitter help center (Twitter, n.d.): An authorized dependent or representative may request the deactivation of the Twitter account (+death certificate, obituary, various documents proving identity and authorization). Deactivated accounts are deleted after 30 days.
	+	-	-	-	-	+	-	Funds are paid out (heir, executor)	-	No published practice: The dependent or executor may report the death of a user to the responsible PayPal customer service (+notarized proofs of death and authorization to prevent fraud). If approved, the account will be closed. If there are funds in the PayPal account, a cheque will be issued in the account holder's name.

Figure 2. The practices of platform providers for handling the case of a deceased account holder

The majority of online platform providers, however, do not seem to see any need to address the issue by publishing relevant regulations. Member mortality rates or the proportion of “dead” profiles are not analyzed, and only a few providers actually delete inactive accounts.

One explanation for this is the declining cost of storage. At the same time, the general legal requirements do not really provide a stable basis for formulating uniform, legally enforceable provisions for the death of a user. The case of Justin Ellsworth, a US soldier killed in action in Iraq, illustrates just how shaky the ground beneath the regulations of platform providers can be when there is a conflict. Ellsworth's parents went to court and were successful in their fight for access to their son's Yahoo! e-mail account after Yahoo! had refused their request, citing their terms of service and the deceased person's right to privacy (BBC Online, 2005).

Thus, platform providers need to deal with the conflicting requirements of data protection provisions, dependents, and the personal rights of the deceased users. In times when platform providers are being watched closely and have to continually update their terms of use and their data use policies for living users, such problems are obviously not a top priority. Figure 2 provides an overview of practices currently in use by major international and European Internet platform providers. These practices cover a wide spectrum of applications, which clearly shows how different such practices can be as well as what a high level of Internet competence and persistence they sometimes require on the part of the user.

5. EXISTING SOLUTIONS FOR DEALING WITH DIGITAL ESTATES

There are ways and means of dealing with the digital estate of a deceased Internet user which already exist (Table 3). Whether these measures are legally enforceable in cases of conflict (inheritance disputes, conflicts with platform providers, or conflicts of the law) and what obstacles must be overcome for the disposition of a legal estate to be legally binding, depends on the respective legal framework and is subject to legal analysis of the applicable law and jurisdiction (Brucker-Kley e.a., 2013).

Table 3. Options for digital estate planning and the execution of a will

Digital Estate Planning Options	Purpose and Benefits	Drawbacks
Leaving access data and instructions with a person of trust	<ul style="list-style-type: none"> ➊ Simple ➋ Relevant for users making provisions in situations involving a severe illness or the anticipated loss of mental capacity 	<ul style="list-style-type: none"> ➌ Beneficiaries have access to the user's data while he/she is still alive ➍ Access data can become outdated or obsolete
Disposing of the digital estate in a conventional will and appointing an executor	<ul style="list-style-type: none"> ➎ Increases the probability of the will being executed ➏ Formal requirements are met ➐ Recommended, in particular in the case of content which is protected by copyright and thus of some relevance in terms of succession law ➑ May increase the enforceability of instructions 	<ul style="list-style-type: none"> ➒ Data covered by personal rights, which end with a person's death, may be of no relevance in terms of succession law ➓ Deposited access data can become outdated or obsolete ➔ Media-friendly wills in electronic format are generally not yet legally recognized

PASSING AND PASSING ON IN THE DIGITAL WORLD – ISSUES AND SOLUTIONS FOR THE DIGITAL ESTATE

Digital Estate Planning Options	Purpose and Benefits	Drawbacks
Digital estate planning services (e.g. SecureSafe, LegacyLocker)	<ul style="list-style-type: none"> ➊ Transparency and access: Enables user to store information on existing Internet accounts including access data and instructions in the event of his/her death ➋ Governance by depositing access data, i.e. less need to depend on platform provider ➌ Privacy: If the digital estate planning service acts as executor of the user's will, data may be deleted without being passed on to dependents ➍ Expertise of the service in the areas of estate planning, execution of wills, and practices of platform providers 	<ul style="list-style-type: none"> ➊ The digital estate planning service may no longer exist at the time of the user's death ➋ Accumulation of access data may constitute a security risk ➌ A person appointed as the executor of the user's will needs to be instructed ➍ Access information may become outdated or obsolete ➎ The dispositions and instructions regarding beneficiaries may not meet the formal requirements of a legal will (e.g., holographic will or public certification)
Password safes (local software, browser, USB, or on the Internet)	<ul style="list-style-type: none"> ➊ Access data remains up to date if the user is consistent in maintaining it in a password safe while he/she is alive 	<ul style="list-style-type: none"> ➊ Does not address the problem of succession. Dependents must be given access to the password safe and master password ➋ Accumulation of access data may constitute a security risk ➌ Documents or instructions can usually not be left in an ordinary password safe
Digital legacy services (e.g., 1000memories, VirtualEternity)	<ul style="list-style-type: none"> ➊ Helps to preserve important memorabilia (e.g., photos, music, texts) by allowing the user to specifically select them while he/she is still alive and thus make them accessible to his/her dependents 	<ul style="list-style-type: none"> ➊ Only relevant for a small portion of a user's digital estate. Does not address the problem of succession of/access to the major portion of the digital estate
Farewell message/e-mail/tweet services	<ul style="list-style-type: none"> ➊ Allows the user to leave a farewell message which is mailed out after his/her death 	<ul style="list-style-type: none"> ➊ Does not address the problem of succession/access
Archives/downloading Internet data (e.g., SocialSafe, dataliberation.org)	<ul style="list-style-type: none"> ➊ Local backup or synchronization of Internet data (profiles, e-mails, contacts) ➋ May allow dependents to access the data through the user's end device 	<ul style="list-style-type: none"> ➊ Data quickly become outdated or obsolete if they are not synchronized periodically ➋ Does not address the problem of access to or removal of Internet accounts

5.1 Digital Estate Planning Services

A digital estate planning service ensures that a digital estate is transparent and accessible. It supports the user's digital estate planning concept by storing the following information deposited by the user while still alive:

1. Access details (username and, usually, a password) for Internet accounts (Facebook, Gmail, etc.) as well as other password-protected online data;
2. Instructions or wishes indicating what is to happen to a specific account/profile/set of data in the event of the user's death;
3. Names of persons of trust who will notify the service of the user's death, be sent the access details, and carry out the wishes deposited by the user.

These basic functions are shared by most existing digital estate planning services. However, there are variations in how they are implemented by the providers. These variations fall into one of the following categories:

a. Type of data or information deposited:

In most cases, the name and the URL as well as the user name and password of an account are encrypted and deposited. Certain services only allow users to deposit the user name or the e-mail address linked to the account in question. If a complete set of login data can be deposited, access for the beneficiaries in the event of a user's death is a straightforward matter, provided passwords are continuously kept up to date. However, the service's safeguard measures must be examined critically, since the storage of all passwords in one place presents a serious security risk.

In addition to the depositing of access details, some services (such as Swiss provider SecureSafe) also enable users to deposit data files. The focus is on providing a service for everyday use as a secure online storage facility for the safe exchange of critical documents, e.g., with banks and the authorities. A user can also nominate beneficiaries who will receive files and passwords in the event of an emergency or death. In this particular business model, data inheritance is not the service's value proposition but rather an added benefit.

b. Responsibility for the execution of the will

In the case of Dutch provider Ziggur.me, the "keep private" function enables customers to keep the existence of certain accounts from dependents in order to protect their privacy. If a customer wants to ensure that such an account is deleted upon their death, the provider acts as the "digital executor" of their will. Providers like Legacy Locker or SecureSafe expressly state that they do not act as executors; the safety mechanisms on which their services are based prevent any access to the deposited access data. In such cases, the executors are the persons of trust whose names have been deposited and who have been advised of their role while the user was still alive. Beneficiaries do not have to be next of kin or friends; other people entrusted with an estate, such as an attorney, can also be nominated and instructed to handle the digital execution of a will.

c. Procedure following the death of a user

In the event of the death of a user, the estate service must be notified. Once it has received the information, it grants the nominated beneficiaries access to the deposited access details and instructions to execute the will of the deceased. The services currently available use one of the following three means of initiating the digital inheritance:

1. The person of trust reports the death to the digital estate planning service, e.g., by **submitting a death certificate** or another official document. Some digital estate planning services, e.g., Legacy Locker, require two persons of trust to confirm the user's death independently.
2. The digital estate planning estate service has an **arrangement with an authority or a public registry**, which registers the existence of a digital estate plan and notifies the service when a customer dies. Swedish provider My Web Will, which is no longer active, had such a cooperation agreement with the Swedish citizens register.
3. A trusted person receives an **activation code** from the customer of the data inheritance service (e.g., SecureSafe), as well as instructions on how to proceed in the event of the user's death. When the user dies, the trusted person logs onto the service's website, enters the code, and thereby activates the data inheritance process.

Usability and **security** are key criteria for a digital estate planning service; however, the basic requirement of such a service is that it will still exist at the time of the customer's death. Entrusting digital estate planning to a startup company which folds after only a few years will result in data being destroyed or, at best, transferred to another company. A service may also suddenly go offline and no longer be available. In such a case, the location of the data is uncertain, and the monthly, annual, or even lifelong fees will have been made in vain. Therefore, the sustainability of the business model and the size of the company may be indicators of a service's **reliability and chances of survival**.

"The Digital Beyond" portal provides a list, which is not intended to be exhaustive, of digital estate planning services, last e-mail services, and online memorial sites that operate internationally in this relatively new business segment (The Digital Beyond, 2012). The 16 listed services which offer digital estate planning were mostly set up between 2008 and 2010. In 2011, only two new providers were added. Three of the providers listed have already discontinued their service, were acquired by another company, or are offline pending re-release. It appears that the first wave of startups is over and a certain amount of disillusionment and consolidation has set in. If a digital estate planning service is not part of a larger range of services, which **adds value while the users are still alive**, or if there is no backing from an investor or a parent company, survival seems to remain difficult, especially in Europe and in domestic markets.

6. CONCLUSION: AN INTEGRATED PERSPECTIVE ON DIGITAL ESTATE PLANNING AND PROTECTION

The analyses of the existing options and legal requirements show that digital estate planning and will execution alone do not constitute a satisfactory solution. A more comprehensive perspective is required which needs to incorporate all aspects of a digital estate and which provides effective solutions that are sustainable in the long term (Figure 3).

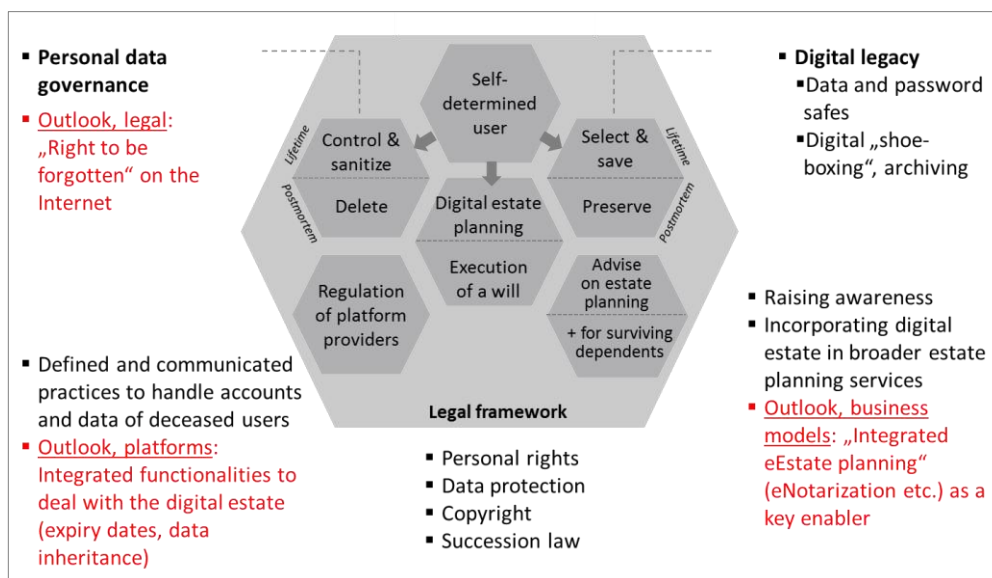


Figure 3. Extended solution space for the digital estate

▪ **Personal data governance**

Loss of control over personal data already begins while we are still alive. Effective, practical solutions must therefore be implemented in the course of our “digital daily lives” to help us organize and control our personal data. Self-determined users make use of practical measures (such as browser settings or web filters) to protect personal data and to avoid leaving a data trail on the Internet.

▪ **The “Right to Be Forgotten”**

The need to select, secure, and preserve data as “digital memories” beyond death may conflict with the demand for the “Right to Be Forgotten on the Internet”. Practical solutions to implement the “Right to Be Forgotten” in our daily Internet usage such as expiration dates for Internet data (Mayer-Schönberger, 2011) or digital erasers like X-pire are still far from being commonly known or used. The issues of lifespan and the protection of Internet data are not primarily technological, although technologies can be a useful means of improving the enforceability of the “Right to Be Forgotten” on the Internet, provided they are practical in their implementation. This corresponds to the principle of “privacy by design” (Cavoukian, 2009), which is also postulated in the strategy paper “A Digital Agenda for Europe” (European Commission, 2010). This principle calls for the right to have personal data protection and privacy embedded in the whole lifecycle of information technologies and information, from their creation to their elimination. Such a concept not only requires commitment and initiative on the part of Internet users and technology providers, but it also calls for the examination and, if necessary, revision of legal provisions.

- **Digital legacy**

In view of the enormous amounts of data that are accumulated in the course of a lifetime, there is an increasing need for bookmarking important content or for keeping it in a special place. The more relevant a digital identity becomes, the more likely a person will look for practicable ways to leave behind a momentous and well-ordered digital legacy. In addition to Internet safes for important documents and passwords, there are specialized digital legacy services that help document key events in a person's life (e.g., 1000memories, VirtualEternity). Other solutions include download or synchronization options offered by platforms or specialized providers (e.g., SocialSafe). These enable users to backup Internet data or social media profiles.

- **Responsibilities of platform providers**

Although self-determination and individual responsibility of Internet users is at the heart of any workable solution, platform providers must still be held accountable to some degree. Guidelines on how to proceed in the event of the death of a subscriber must be put in place and communicated to users. At this stage, however, there is little motivation for platform providers to address this issue. Moreover, the existing legal framework does not really provide a sound foundation for uniform, binding regulations. Nevertheless, providers will have to start incorporating effective measures into their platforms and data use policies in order to control the life cycle of accounts and data (e.g., expiry dates, data inheritance, and prearrangements for inactive accounts). Google's Inactive Account Manager, launched in April 2013, is a step in this direction (Google, 2013).

- **Raising awareness and offering support**

Since digital estate planning is still in its infancy and the relevant regulations put in place by platform providers are diverse and often insufficient, there is a great need for advisory services to provide information on digital estate planning and to assist the surviving dependents after a death has occurred. These services can take the form of helping the next of kin to identify and handle a digital estate (as offered by German service provider Semno, which identifies digital estates by analyzing the personal computing devices of deceased persons), or they can include providing explanations/information by public authorities (e.g., data protection authorities, civil registry offices) or private service providers. For notaries, attorneys, financial services consultants, and other estate planning service providers, incorporating digital estate planning into their services might represent an interesting extension of their fields of business.

- **Legal framework**

The question of how to treat a person's digital data after their death has various legal ramifications. For one, the problem must be examined from the perspective of succession law: Can data be inherited? Can data be disposed of in a will? Next, an individual's personal rights need to be considered: How can the rights of a person be protected beyond their death. What options do the next of kin have? Some protection is provided by personal data protection regulations; however, the question remains whether there should be rules that determine how the data of the deceased must be dealt with and if the "Right to Be Forgotten" on the Internet can be enforced.

REFERENCES

- Avok, M., 2012. *Legislators ponder whether Facebook account should be part of your estate*. Associated Press [WWW Document]. http://www.boston.com/business/technology/articles/2012/03/16/is_facebook_part_of_your_estate_new_laws_debated/
- BBC Online, 2005. Who owns your e-mails? [WWW Document]. http://news.bbc.co.uk/2/hi/uk_news/magazine/4164669.stm
- Brucker-Kley, E., e.a., 2013. *Sterben und Erben in der digitalen Welt*. vdf Hochschulverlag an der ETH Zürich. <http://www.vdf.ethz.ch/vdf.asp?isbnNr=3545>
- BFS-1-Bundesamt für Statistik. *Statistik der Bevölkerung und der Haushalte (STATPOP)*. Downloaded from STAT-TAB , *Ständige Wohnbevölkerung der Schweiz nach Alter*, as per April of each year. [WWW Document]: <http://www.pxweb.bfs.admin.ch> (last accessed October 2013)
- BFS-2-Bundesamt für Statistik. *Todesfälle nach Alter 1970-2012*. [WWW Document]: <http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/06/blank/data/01.Document.67397.xls> (last accessed October 2013)
- Cavoukian, A., 2009. *Privacy by design*. Office of the Information and Privacy Commissioner. Ontario.
- The Digital Beyond, 2012. *Digital Death and Afterlife Online Services List* [WWW Document]. <http://www.thedigitalbeyond.com/online-services-list/>
- European Commission, 2010. *A Digital Agenda for Europe* (No. COM(2010) 245 final/2). Brussels.
- Facebook, n.d. *How do I report a deceased person or an account that needs to be memorialized or deleted?* | Facebook Help Centre [WWW Document]. <https://www.facebook.com/help/150486848354038/?q=deceased&sid=0NZeIqyvUCr0HFG1p>
- Google, 2012. *Accessing a deceased person's mail - Gmail Help* [WWW Document]. <https://support.google.com/mail/answer/14300?hl=en&topic=1669055&ctx=topic>
- Google, 2013. *Inactive Account Manager* [WWW Document]. <https://www.google.com/settings/u/0/account/inactive>
- Lustig, N., 2010. *How We Calculated That Three Facebook Users Die Every Minute*. [no longer available online]
- Lustig, N., 2012. *2.89m Facebook Users Will Die in 2012, 580,000 in the USA* [WWW Document]. <http://www.nathanlustig.com/2012/06/06/2-89m-facebook-users-will-die-in-2012-580000-in-the-usa/>
- Mayer-Schönberger, V., 2011. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.
- SocialMediaSchweiz.ch. *Facebook - Die Schweiz in Zahlen (Updates pro Stichtag)* [WWW Document]. http://www.socialmediaschweiz.ch/html/ch_fb_publicationen.html (last accessed October 2013).
- Twitter, n.d. Help-Center | *How to Contact Twitter About a Deceased User* [WWW Document]. <http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/87894-how-to-contact-twitter-about-a-deceased-user#>
- Yahoo!, 2012. *Yahoo! Terms of Service* (Status: 16.3.2012) [WWW Document]. <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html>
- ZHAW, School of Management and Law, 2012. *Sterben und Erben in der digitalen Welt*. Project Website [WWW Document]. <http://zwi.zhaw.ch/digitalessterben>