
DOI
https://doi.org/10.1016/j.clsr.2018.04.008

Document Version
This is the Accepted Manuscript version. The version in the Universitat Oberta de Catalunya institutional repository, O2 may differ from the final published version.

Copyright and Reuse
This manuscript version is made available under the terms of the Creative Commons Attribution Non Commercial No Derivatives licence (CC-BY-NC-ND)
http://creativecommons.org/licenses/by-nc-nd/3.0/, which permits others to download it and share it with others as long as they credit you, but they can't change it in any way or use them commercially.

Enquiries
If you believe this document infringes copyright, please contact the Research Team at: repositori@uoc.edu
How do we provide the digital footprint with eternal rest? Some criteria for legislation regulating digital wills

Agustí Cerrillo-i-Martínez

Law and Political Science Department, Universitat Oberta de Catalunya, Barcelona 08860, Castelldefels, Spain

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Digital footprint
Digital wills
Digital service provider
Regulation

ABSTRACT

This article analyses the implications of the death of digital service users on their digital footprint and assesses some of the solutions—contractual and legislative—that have been posited to date by digital service providers and by Parliaments of a few countries. In view of the different initiatives analysed, and the experience gained in their implementation, the paper presents legal certainty, effectiveness and transparency as criteria that should guide the regulation of the digital footprint in the case of death. These criteria must allow for the adoption or regulation of mechanisms for managing the digital footprint of digital service users to be clear and trustworthy for them and efficient and easily recognized and adopted by digital service providers.

© 2018 Professor Agustirillo-i-Mart. Published by Elsevier Ltd. All rights reserved.

1. The digital footprint

A person’s digital footprint is made up of all the records that are in the cloud. They are created when they communicate with others on the Internet via email, when they take part in social networks, when they store things, when they share photos or videos, or when they read books, listen to music, watch films, play games or make purchases from online stores through digital service providers. Also forming part of one’s digital footprint are the accounts on digital service providers used to manage all these records (Varnado, 2014).

The content of the files making up the digital footprint differ in nature and value. Some of these records may contain data protected by different rights, some of them fundamental, such as freedom of expression, secrecy of correspondence, personal data protection, image rights and the right to personal and family honour. Others may contain original creations protected by intellectual property rights (i.e. documents or photos). Furthermore, both of these types of records

1 I have chosen to use the term “digital footprint” in this article. Nevertheless, it should be noted that a review of the literature reveals the use of other expressions, such as digital property (Watkins, 2014; Connor, 2010); digital assets (Connor, 2010; Edwards & Harbinja, 2013; Hopkins, 2013); digital traces (Wright, 2014); digital estate (Hopkins, 2013); digital legacy and digital memory (Bassett, 2015) or digital remains (McCallig, 2013).

2 This very broad definition of the digital footprint has led one author to acknowledge that its application is “utterly mindboggling” (Ray, 2012). Nevertheless, we cannot ignore the fact that some authors regard this broadness as useful, to be able to include everything that actually has to be regarded as part of the digital footprint (Connor, 2010).

https://doi.org/10.1016/j.clsr.2018.04.008
0267-3649/© 2018 Professor Agustirillo-i-Mart. Published by Elsevier Ltd. All rights reserved.

Please cite this article as: A. Cerrillo-i-Martínez, How do we provide the digital footprint with eternal rest? Some criteria for legislation regulating digital wills, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018),
may have an economic value, to a greater or lesser degree (i.e. bitcoins or money earned on an online gaming site). Others, meanwhile, may be—only or additionally—of sentimental value to the user or their personal or family circle (i.e. correspondence carried out by email, photos shared on family albums uploaded onto the web or playlists or reading lists shared with him or her). Some, such as emails, may even be of value greater to that inherent in them, as master keys that allow users to manage their digital footprint in digital services, in saving the data necessary to access them (Carroll & Romano, 2010, 109).

The footprint created by users’ Internet activities is stored on digital service providers’ servers in the cloud, which are generally managed through password-protected accounts.

Whilst users are still alive, their digital footprint is, formally at least, under their exclusive control by means of the personal access provided by the digital service provider.

However, when they die, they lose this control. First of all, when a digital service user dies, their digital footprint remains on the Net if nothing is done about it (Carroll & Romano, 2010; Watkins, 2014).

It is not just that. When a user dies, their successors, relations and friends often find it impossible or difficult to manage the files making up the former’s digital footprint, whether in terms of deleting it, accessing it or keeping it alive.

This situation has led to a range of lawsuits in recent years that have concluded with a number of court rulings in some countries that have had great media impact.

For example, one might recall the case of the parents of a soldier killed in Iraq who wished to access the emails sent by their son from the front, to create a memorial to him, which Yahoo refused until access was granted by a judge (Lastokwa, 2010). There is also the tale of a Virginia family who sought, in vain, to access the Facebook profile of their son, who had committed suicide at the age of 15, to investigate the circumstances that had led to his death (Varnado, 2014; Watkins, 2014).

These and other issues that have arisen over recent years have led some digital service providers, although initially reluctant to do so, to make changes to their policies to provide a response to this new reality. The social pressure often accompanying these lawsuits has meant that different rulings have begun to adopt some legislation with mechanisms enabling management of a deceased user’s digital footprint. It is easy to appreciate how, as McCallig points out, “a bereaved family in dispute with Facebook often makes a national or international news story” (McCallig, 2014).

Digital service providers have no incentive a priori to do anything with regard to managing the digital footprint of dead users, in that they generally base their business model, the free-of-charge nature of their services, on the use they make of the information generated by their living users’ activities. This is why doing anything with regard to deceased users’ digital footprints would normally entail spending time and money with, probably, little return (Varnado, 2014; Leaver, 2013).

Nevertheless, some digital service providers, aware of the need to provide a response to this situation, have begun to amend their policies to include specific rules on the matter or to offer options for users to electronically express their preferences in this regard. Additionally, recent years have seen the appearance of companies offering to manage the digital service accounts of deceased users. Furthermore, in this scenario, the doubt arises as to whether current legislation is enough to provide an answer to the challenges presented by digital footprints when users die (Edwards & Habbinja, 2013). Therefore, to provide a global and comprehensive response to the different situations that may arise with regard to digital footprint management subsequent to a user’s death, some countries have begun to adopt legislation incorporating digital footprint management mechanisms.

Nevertheless, we cannot ignore the fact that digital footprint management is still not a generalized social concern, despite the stories appearing in the media. Indeed, a US survey shows how 63% of Americans make no plans for their digital footprint after their death. These figures are particularly significant when noting that, according to a YouGov survey in the UK, only 20% of the young people aged between 18 and 24 surveyed have ever considered the matter.

Whatever the case, there is no doubt that this concern will grow as digital natives get closer to death and the presence on the Net expands and evolves with the appearance of new digital services or new social uses of information and communication technologies (McCarthy, 2015). Indeed, the problem has only just begun and digital footprint management will surely...


become a more pressing issue as digital natives age and their
digital footprint expands (Varnado, 2014; Kutler, 2011).

We cannot ignore the fact that, according to some media
estimates, by 2012, there were 10 million Facebook profiles of
people who had died and, by the year 2098 there will be more
dead people than living ones on this social media network.7

The lack of proper mechanisms for managing a dead per-
son’s digital footprint could have a wide variety of serious im-
plications. However, we should note at the very start that dig-
ital footprint management needs to take account of the fact
that, beyond the interests of deceased users’ successors and
family, there may be other rights or interests in play.

This article analyses the implications of the death of dig-
tal service users on their digital footprint and assesses some
of the solutions—contractual and legislative—that have been
posited to date.

To do this, it is organized into four sections. The first sets
out some of the solutions that digital service providers are of-
fering. The second section analyses legislation adopted by the
United States and France in response to the issue. The third
section studies the legislation adopted in Catalonia in this re-
gard. Lastly, the fourth section details the criteria that should
govern the adoption of digital footprint management mecha-
nisms when a service user passes away.

2. Digital footprint management initiatives

The majority of a digital footprint is controlled by digital ser-
vice providers via their terms of service agreements, and the
policies governing the provision of most digital services gen-
erally establish the use that can be made of the records cre-
ated by the activities carried on by users (Edwards & Harbinja,
2013).

Nevertheless, the agreements, terms of reference or poli-
cies of these service providers do not generally specify what
happens to digital footprints once users are deceased: if they
are to be deleted, retained or access provided thereto. Nor do
they specify the options available to successors, family mem-
bers or friends in this regard.

As a starting point, one might highlight the fact that, in
most cases, agreements with digital service providers do not
establish maximum terms of enforceability, nor do they in-
clude clauses on the impact that the user’s death may have
upon the agreement.8 However, some providers do indeed ex-
plicitly contemplate in their agreements that the user’s death
implies termination thereof (with the so-called “No Right of
Survivorship” clauses) (Watkins, 2014).9

What’s more, in most cases, the user’s relationship with the
service providers is based on highly personal (intuitu personae)
agreements,10 meaning that there is no right to subrogation
for their successors in such agreements. After their death, the
person disappears and the personal rights to which they held
title are extinguished. All these highly personal agreements
with digital service providers terminate upon the death of the
user.11 They cannot, therefore, be subject to mortis causa trans-
fer.

Additionally, the identification and authentication applica-
tions and mechanisms that were under the user’s exclusive
control to access the digital services are not transferrable, in
principle, to his or her successors.12 Indeed, according to some
legislation, doing so could potentially constitute a usurpation
of civil status or improper access to information systems.13

So it is that, as things currently stand, the deceased’s suc-
cessor, family and friends cannot access either user contents or
accounts to manage them. Indeed, these and other matters
do not form part of the contractual relations with digital
service providers and so, in principle, they have no right to
manage the digital footprint of the deceased user (Edwards &
Harbinja, 2013). Nor may they use the passwords or applica-
tions as if the users had not died.

Given this, in recent years, digital service providers have
been pushing through changes to their policies so that their
users might be able to place on record how their digital foot-
print is to be managed after their passing. With these changes,
providers are seeking to deal with the growing social demands
regarding the accounts of deceased users and the administra-
tion of the records created by their activities or those stored
on the formers’ databases.

Alongside these changes to digital service providers’ policy,
a number of services have been surfacing, offered by different
kinds of companies, which aim to help the deceased, or their
successors or families, to manage their digital footprint.

Set out below is a brief analysis of the policies of leading
digital service providers on managing the digital footprint of
their users after death. Also detailed are the main private ini-
tiatives that have arisen as a response to this situation.

2.1. Leading digital service providers’ policies on deceased
user accounts

Leading digital service providers and social media networks
in particular, are modifying their policies and terms of service

---

7 Griffin, A. (7 March 2016) “Facebook will have more dead people than living ones by the end of the century, researcher claims”. The Independent. Available at: http://www.independent.co.uk/lifestyle/gadgets-and-tech/news/facebook-will-have-more-dead-people-than-living-ones-by-the-end-of-the-century-researcher-claims-a6917411.html (last consulted August 2017).

8 However, one should not ignore the fact that some licences over digital books or music do state explicitly that they are time-
limited [Edwards, 2013 #8346].


10 This is the case, for example, with Facebook, in Clause 4.8 of its Statement of Rights and Responsibilities, which states that Facebook users will not share their passwords or let anyone else access their account. Accessible as: https://es-es.facebook.com/legal/terms/update (last consulted August 2017).

11 Catalonia’s Civil Code states that a person’s “civil personality” is extinguished with their death (Art. 211-1).


13 See, for example, Article 401 of Spain’s Criminal Code. In the US, third-party access to an account could be grounds for bringing a cybercrime lawsuit, pursuant to federal law (Watkins, 2014).
agreements to include mechanisms for managing digital foot-
prints after a user’s death.

It should be emphasized that these are often agreements
for which consent is provided by clicking on a box (clickwrap
agreements) or by scrolling down the agreement (browsec-wrap
agreements), whose users do not generally read their contents
(Fernández Flores, 2015). Above and beyond their acceptance
as an effective mechanism for placing on record user consent
(Dickens, 2007), it is clear that, from the standpoint of this ar-
ticle, users are unaware of the impact all this has on the man-
agement of their footprint after their death.

The impact of digital footprint management goes beyond
the securing of the cancellation of accounts or access to
records. In recent years, we have witnessed how the manage-
ment of the deceased’s digital footprint may also have sig-
nificant effect on the grieving process of family and friends
shared over the Web and, in general, on the process of pub-
lication of the death (Wright, 2014; Bassett, 2015; Sofka et al.,
2012).

Set out below is a brief summary of some providers’ poli-
cies in this regard.

2.1.1. Facebook

To begin with, it should be noted that Facebook’s Statement
of Rights and Responsibilities grants no third-party beneficial
interests.14 What’s more, it states that users accept the un-
dertaking not to share their passwords or let anyone else ac-
cess their account.15 Furthermore, it contains no provision ex-
pressly establishing that the agreement with the user termi-
nates upon the latter’s death (McCullig, 2014).

Nevertheless, Facebook now offers the option that, when
a user dies, their accounts be “memorialized” or definitively
deleted at the proposal of a successor or family member
(Sherly, 2013).

The social media network’s policy on digital footprint man-
agement has evolved since its appearance, as users have de-
manded that the company offer the option that friendships
be linked with content created by the deceased (McCullig,
2014). Indeed, after a campaign by friends of the Virginia Tech
mass shooting of April 2007, Facebook amended its initial pol-
icy of deleting accounts of deceased users after thirty days,
adding the possibility of converting the account into a memo-
rial (Mazzone, 2011; McCullig, 2014; Bassett, 2015). Over the
course of time, the possibility of creating this “memorialized”
page seems to be the most popular option, particularly with
active Web users, such as the young, or users who have died
under violent circumstances (Leaver, 2013).

With the memorialized account, the user’s friends can con-
tinue to post to the former’s page as they had been doing when
he or she was still alive, thus turning Facebook into a space
for managing grief and pain. The wall’s content will be just as
accessible as before, allowing Facebook friends to post mes-
ages and photos and, ultimately, share their grief (McEwen &
Scheaffer, 2013).

The memorialized account is administered by a “legacy
contact” chosen by the user.16 This legacy contact has very
limited administration powers over the account, such as
adding a pinned post to the memorialized profile (e.g. a last
message on behalf of the deceased user), responding to new
friend requests and updating the deceased users’ profile pic-
ture and cover photo. However, they cannot enter into the ac-
count as if they were the user, nor delete or modify anything
posted by the user, nor remove people from their friend list.

Facebook provides the option of the account owner giving
the legacy contact permission to download a copy of what
they have published on their account (such as photos, videos,
profile information, events and friends lists). However, it does
not provide access to other content, such as messages or ad-
verts they may have accessed, unless so provided for in a will
or other valid consent document that contains express
authorisation.17

Removal of the account is contemplated for those cases in
which the user has so stated a preference in the space de-
dicated for the purpose. Facebook also accepts requests for
removal from close family members or executors, provided
they can provide proof of authority and a document placing
the death on record (death certificate, obituary or memorial
card).18

2.1.2. Google

Google’s policy is based on providing account holders with an
“inactive account manager”.19

Using this inactive account manager, users can tell Google
what to do after their account has been inactive for a certain
period.20 The inactive account manager allows them to spec-
ify how long the account shall remain unused before being
regarded as inactive. It also allows them to provide a mobile
phone number or an email address that Google will contact
before taking any action. Lastly, it allows them to choose up to
ten friends or trusted contacts that Google will notify that the
account is inactive.

Google users can specify that their data be shared with
these trusted contacts. They can also indicate that any mes-
ages sent to the inactive account receive an automatic reply.
Lastly, they can tell Google to delete the account when it be-
comes inactive.

Google also allows people to request access to an account
or that a deceased user’s account be deleted. However, in such
a case, Google will review the request and take a decision. This
decision will be made, according to Google, taking into account
its responsibility to keep people’s information safe, secure and

private, meaning it cannot, for example, provide passwords or other login details.  
Lastly, Google has also established a specific procedure for requesting reimbursement of deceased user funds in Google's possession (income from the AdSense program or Google online payment service balances).

### 2.1.3. Instagram

Instagram has a policy similar to Facebook's, allowing a deceased user's immediate family members to notify it of a user's death and either memorializing or removing the account. To memorialize the account, all that is needed is for anyone to provide Instagram with proof of death, such as an obituary or news article.

To remove the account, an immediate family member must provide notice and submit the deceased person's birth certificate, death certificate or proof of authority as legal representative or his/her successor.

### 2.1.4. Twitter

Twitter provides a form for a deceased user's representative or direct family member to request removal of the account. The applicant must provide proof of the user's death. Under no circumstances can access to the deceased user's account be provided.

Twitter also offers immediate family members and other authorized individuals the possibility of removing certain imagery via a form for removing images or videos belonging to the deceased user. Before removing the information, Twitter will consider its public interest and newsworthiness.

### 2.1.5. LinkedIn

LinkedIn allows anyone who becomes aware of the passing of a community member to provide notice of the fact for the account to be closed and his or her profile to be removed.

To do this, they need to fill in a form with the deceased member's name, the URL of their LinkedIn profile, their relationship to the deceased, the date of their passing, a link to the obituary and the company they most recently worked at.

2.1.6. Dropbox

Dropbox has established a procedure to request access to a deceased user's account. To be able to access the account, the applicant must provide by conventional post a valid court order establishing that it was the deceased person's intent that the applicant have access to the files in their account after the person passed away, and that Dropbox is compelled by law to provide the deceased person's files.

### 2.2. Private initiatives for digital legacy management

Aside from these initiatives driven by the digital service providers', recent years have seen the promotion of a range of other private initiatives to provide a response to some of the problems identified. Most of these firms are linked with funeral parlours or insurance companies, although some countries have also seen the appearance of small start-ups in the field.

Some companies offer to manage the deceased's digital footprint, whilst others help users plan what to do with it. Firstly, there are companies that help people decide what is to be done with their digital footprint. These companies improperly use the term "digital will" to refer to the document containing these wishes, which can cover not only the closing of accounts but also access to content and the obtaining of copies of the information stored on digital service providers' servers.

Secondly, there are companies that delete the digital footprint, managing the cancellation of accounts and wiping the deceased person's presence from the Internet.

Thirdly, there are companies that manage accounts and passwords accessing digital services so that, after a user's death, they can be used to execute their last will or to make them available to third parties to administer the account.

In this regard, it should not be forgotten that users have an average of 25 passwords and that they can change over time (McCarthy, 2015).

In fourth place, there are companies offering users the chance to decide how they wish to be remembered when they die, for example by creating sites commemorating the deceased.

Lastly, some insurance companies have recently begun to include new Internet-related benefits in their funeral expense policies. In particular, they include the service of wiping the insured's digital life, giving successors the option of the insurance company removing the insured's profiles from all social media networks, and deleting their blogs and email accounts.

See, for example, Eliminalia (https://eliminalia.com) (last consulted August 2017).

See, for example, Netarius (https://ca-es.facebook.com/netarius/) (last consulted August 2017).

See, for example, Eternime (http://eternime.me) or Lifenaut (https://www.lifenaut.com) (last consulted August 2017).


30 Basset refers to two categories of companies: asset maintenance and posthumous scheduling (Bassett, 2015).

31 See, for example, Tellmebye (https://tellmebye.com) (last consulted August 2017).

32 See, for example, Eliminalia (https://eliminalia.com) (last consulted August 2017).

33 See, for example, Netarius (https://ca-es.facebook.com/netarius/) (last consulted August 2017).

34 See, for example, Eternime (http://eternime.me) or Lifenaut (https://www.lifenaut.com) (last consulted August 2017).
2.3. Assessment of digital legacy policies and services

The leading digital service providers currently offer some kind of mechanism for managing one's digital footprint. By means of self-regulation, the providers generally provide for the fact that, when a user dies, his or her successors or immediate family can request conversion of the account into a memorial or its cancellation. The analysis performed indicates that, despite the similarities identified, there is no one common solution and, often, the options offered by service providers are very different (for example, regarding what can be done when a user has died and the requirements or necessary documentation).

These mechanisms have the advantage of guaranteeing that the users’ decisions about how to manage their digital footprint after dying are applied by digital service providers particularly when they have recorded them in through the service provider system.

However, these mechanisms have some weaknesses too. From the point of view of legal certainty, the majority of mechanisms provided by digital service providers do not guarantee that the users’ decisions will be respected because they tend to allow only cancelling the digital accounts or to memorialize them but not to download a copy of the records. They do not also guarantee their decisions because they only take into account the users’ decisions recorded through the service provider system but not those expressed by other means. Furthermore, as it has previously been stated, digital service providers often put forward third person rights as an impassable excuse to avoid the execution of the users’ decision about their digital footprint.

From the point of view of effectiveness, it is clear that the mechanisms provided by digital service providers will reach the expected results. However, as each digital service provider has its own mechanism and between them, there are several differences, there are important impediments to their effectiveness. In addition, the formalities sometimes are long and costly and they do not fit to the necessities of the deceased person’s family that usually try to look after solving quickly all the issues related to the users’ death.

Finally, from the point of view of transparency we cannot ignore that the majority of these mechanisms are unknown by services’ users. Furthermore, digital service providers do not usually provide specific mechanisms to inform relatives or people named to execute the users’ decisions about what they can do with the digital accounts of the user when they die.

With regard to the initiatives that have appeared, their short lifespan does not allow us to gauge either their viability or their effectiveness. Nor, currently, is there information on the volume of their activities. Indeed, one of the doubts raised concerning these initiatives is their continuity and the consequential guarantee that, when a user dies, they will still be in business.

Furthermore, it has to be added that other problems are also beginning to be detected, ones that could cause suffering or upset the deceased’s family and friends, such as that created by people flooding memorial sites with abusive or offensive content (RIP trolling) or people who did not know the deceased sending messages (grief tourism) (Wright, 2014; Marriott & Ellison, 2012).

The limitations of self-regulation and of the mechanisms implemented by some digital service providers reveal the need to promote new alternatives through regulation by parliaments and public administrations.

3. Digital footprint regulation: experiences compared

Current regulation in most countries permits the finding of mechanisms to regulate a digital user’s footprint by means of, for example, the protection of their personal data, intellectual property, regulation of digital services or even inheritance law (Buitelaar, 2017).

Nevertheless, and without carrying out a specific analysis of the legislation in force in each individual country as differences can be observed between different law systems (Harbinja, 2017), it can be seen that these laws do not specifically contemplate how to manage digital footprints when data owners die. Therefore they cannot provide an adequate complete response to the different problems referred to above.

From the point of view of data protection, it has to be taken into account that when a person dies, he or she does not have a right to protect his or her personal data. That is clearly stated in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC which recognizes that it “does not apply to the personal data of deceased persons” (Recital 27). In the same sense, some State Members regulations (i.e. Sweden, Spain or United Kingdom). However, the Regulation (EU) 2016/679 also states, “Member States may provide for rules regarding the processing of personal data of deceased persons”. In that way, some countries have been recognizing some data protection rights related to death persons (i.e. Bulgaria, France or Estonia) (McCallig, 2014). However, as Harbinja has stated, “the legislation is not harmonised and gives different powers to the heirs and data subjects” (Harbinja, 2013).

From the point of view of intellectual property rights, which are transmissible mortis causa, this would only affect to a part of the user’s digital footprint because only a few records can be considered as intellectual property. As McCallig has stated “once that copyright subsist in a work certain post-mortem rights then become available offering legal protections to both the creator (author) and to the work” (McCallig, 2013). However, other authors have questioned if the extension of intellectual property rights beyond the death of the author has theoretical grounding and if it is justified (Desai, 2011; Subotnik, 2015).

In response to the limitations to manage a deceased person’s digital footprint of these regulations, a few countries have begun to pass legislation specifically regulating how to manage it. This legislation has to deal with the different challenges identified, such as what the digital footprint is, how to record the user’s will and how this is related to third-party rights and, lastly, how these aspects are connected with the
agreements signed with digital service providers or with their
terms of service.

As we shall see below, the ad hoc legislation passed on
digital footprint management is based on three different ap-
proaches: managing the digital footprint as an asset, in the
form of personal data protection and in terms of the will of
the deceased.

In the next pages, three regulations that are an example of
each of these approaches will be analysed. First, this section
will outline the main features of the legislation adopted by the
United State where digital footprint is regulated as an asset
and France where digital footprint is regulated from the point
of view of data protection. Secondly, in the following section,
one will focus its attention on the regulations implemented in
Catalonia where digital footprint is regulated as an expression
of the user’s last will.

3.1. Regulating the digital footprint as an asset: the case
of the United States of America

Federal legislation in the US does not specifically regulate
management of the digital footprint, although the matter is
subject to some laws such as the 1986 Electronic Communi-
cation Privacy Act (ECPA, Section 2702(b)), the Stored Com-
munications Act (SCA, Sections 2701-2712), and the Computer
Fraud and Abuse Act (CFAA, Section 1030) (Watkins, 2014).

However, individual states have, within the framework of
their powers, regulated digital footprint management, with
Oklahoma being the first to do so in 2010. Today, 39 states
have adopted “digital estate planning” legislation. In general
terms, digital footprint is regulated in the US as an asset which
means that it can be managed using the same mechanisms
used to manage other assets.

In particular, an overall analysis of the legislation adopted
in the US on the matter indicates the coexistence of two regu-
latory models with quite different approaches. These models
are based on the proposals made by the National Conference
of Commissioners on Uniform State Laws and by NetChoice,
representing the service provider industry. The two models
have different approaches and offer different solutions to dig-
ital footprint management in the case of death.

One the one hand, the Uniform Fiduciary Access to Digital
Assets Act (UFADAA), promoted by the National Conference of
Commissioners on Uniform State Laws, of which two versions
are available (2014 and 2015), has been or is in the process of
being adopted by 24 states.36

According to the UFADAA, digital assets are electronic
records in which individuals have a right or interest.37 The
UFADAA seeks, firstly, to give fiduciaries the legal authority
to manage digital assets and electronic communications in the
same way they manage tangible assets and financial accounts.

Secondly, it gives digital service providers legal authority to
deal with the requests they may receive, while respecting the
user’s reasonable expectation of privacy.

This model seeks to give Internet users the power to plan
the management and disposition of their digital assets in the
same way as they can with their tangible ones. To this end,

36 The latter version of the Revised UFADAA has been welcomed
https://doi.org/10.1016/j.clsr.2018.04.008
In addition to the legislation adopted, one cannot ignore the role played by the courts with regard to digital footprint management (Watkins, 2014).

3.2. Regulating the digital footprint as protection of the deceased’s data: the case of France

From a different perspective, in France, digital footprint is regulated as personal data which means that it can be managed using some of the mechanisms used to protect them.

Within Europe, the first legislation to be adopted on the matter was France’s Law no. 2016-1321, of 7 October 2016, for a Digital Republic (the “the Digital Republic Act”), modifying Law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties.

The Digital Republic Act contains provisions on the management of deceased persons’ personal data. To begin with, it recognizes that people’s rights with regard to the processing of personal data expire with the death of their owner. Nevertheless, they may remain provisionally in force for managing their digital footprint. In this regard, it contemplates the option of arranging during one’s lifetime the conditions for conserving and communicating personal data after one’s death.

Each individual can, by means of instructions, establish how they wish their data protection rights exercised when they die. These instructions may cover the retention, deletion or disclosure of their personal data after they die. Should the data they wish to disclose include third-party personal data, an account should be taken of the general provisions of personal data protection legislation. These instructions can be changed at any time.

Firstly, the option is contemplated of adopting general instructions on the person’s personal data as a whole. These instructions can be registered with “digitally trusted” third parties certified by the country’s National Commission for Information Technology and Civil Liberties (CNIL).

Secondly, there are specific instructions on the processing of personal data. These instructions are aimed at data controllers. They are subject to the express consent of the interested party and cannot arise solely from their acceptance of the general terms of service.

In their instructions, users can appoint a person responsible for executing them. When this person becomes aware of the user’s passing, he or she can discover the content of the instructions and request that the data controllers implement them. If no such person is appointed or, unless there is an instruction to the contrary, the appointee has also passed away, the user’s successors are entitled to acquaint themselves with the instructions and request that the data controllers implement them.

Any agreements signed with digital service providers limiting the prerogatives recognized in the Act shall be regarded as not entered into.

If there are no instructions or there is no statement to the contrary in the instructions themselves, the successors may exercise the rights contemplated in the law after the user’s death to arrange and settle the deceased’s estate or to notify the data controllers of the user’s death. Additionally, the successors may request that the data controllers close the user’s accounts, oppose the continued processing of the deceased’s personal data or request that they be updated, of which the data controller must render account.

Lastly, it provides that digital service providers must inform users of the personal data in their possession and must offer them the choice of whether or not to disclose this data to a third party appointed by the latter.

4. Regulating the digital footprint as an expression of the deceased’s last will: the case of Catalonia

Law 10/2017, of 27 June, on digital wills and the amendment of Books Two and Four of the Catalan Civil Code (the “Digital Wills Act”) has a different approach to regulating the digital footprint to that taken by either the United States or France. The Catalan regulation of digital footprint is based on the recognition of the deceased’s last will. Amongst other reasons, this is due to the powers held by Catalonia as an “autonomous community” of Spain.

Set out below are the powers of the Government of Catalonia, followed by an analysis of the Digital Wills Act.

4.1. The powers of the administration of the government of Catalonia with regard to the digital footprint

As we have seen above, regulation of the digital footprint can be tackled from the perspective of legislation on digital services or that on data protection. In Catalonia’s case, the issue has been regulated within the framework of civil inheritance law.

Firstly, with regard to telecommunications, Catalonia’s Statute of Autonomy only provides that Catalonia has powers over buildings’ conditions for the installation of shared telecommunications infrastructures, respecting Spanish State legislation on telecommunications (Art.137.2). It also states that Catalonia has powers over the inspection of shared telecommunications infrastructures and the exercising of the associated penalty-imposing powers and administration of the register of shared telecommunications infrastructure engineers and of the register of multiplex managers (Art.140.7.a and b). Autonomous community-level powers on the matter are very limited and closely linked to infrastructures rather than services.

Secondly, with regard to personal data protection, Catalonia’s Statute of Autonomy establishes only that Catalonia has executive powers in the field of personal data protection, whilst respecting the guarantee of fundamental rights with regard to this issue (Art. 156). It therefore does not have the

---

46 Article 40.1.II.
47 Article 40.1.II.
50 Article 40.1.II.
51 Article 40.1.II.
52 Article 40.1.II.
53 Article 40.1.III.
54 Article 40.1.IV.
power to regulate the digital footprint based on this power, as France has done. On the other hand, Article 129 of the Statute states that Catalonia has exclusive powers in the field of civil law. The provisions of Article 149.1.8 of the Spanish Constitution limit this power. According to the precedent set by Spain’s Constitutional Court, autonomous community powers must be exercised with regard to the “conservation, modification and implementation” that constitute the limit of the attributable and exercisable powers (Judgment 31/2010). In particular, the Court had previously held that “the Constitution permits that pre-existing special or local civil rights may be the object not just of ‘conservation’ and ‘modification’, but also of legislative action that enables their organic growth, thereby acknowledging not only the historical nature and current enforceability, but also the future vitality of said preconstitutional regulations”. According to the Court, it “permits the legislative regulation of fields previously not governed by the Law” (STC 88/1993, FJ 3).

Finally, Catalonia has also exclusive powers on administrative organisation and mechanisms of public activity (Art.150).

4.2. The Digital Wills Act

The Digital Wills Act amends a number of precepts of Catalonia’s Civil Code to acknowledge that people can place their digital wills on record in the case of their death. Digital wills, in the case of death, are the provisions established by a person so that, when they die, their successor or executor, or the person appointed to execute them, may act before those digital service providers with whom the user has an active account. Digital service users may place on record the content and the scope of the tasks to be performed. These tasks may include a range of steps, including notifying digital service providers of the death of the user, requesting that digital service providers cancel active accounts, requesting that digital service providers execute contractual clauses or activate policies established in the case of a user’s death and, if applicable, that they issue a copy of any digital records on their servers. It is interesting to note that the Digital Wills Act contemplates that those responsible for executing the digital wills may not have access to the contents of the accounts or the digital records unless the user so establishes in their will or a court order to the effect is secured. Any costs arising from the execution of the digital will be borne by the estate, unless the testator has indicated otherwise.

Additionally, digital wills can also appoint the person responsible for executing them. This person may be either a successor or any other person named by the testator. The appointee can also be a legal person, e.g. a digital estate management company. The digital will testator may indicate the natural or legal person(s) who are to be informed of the existence of the digital will upon the former’s death. In the absence of any such express appointment, execution of the digital will shall fall to the successor, executor or personal representative of the estate, who may execute the digital will or appoint another person to execute it. The person responsible for executing the digital will does not have any minimum attributed powers, as these shall in any case be established by the content of the digital will itself.

Digital wills and the person responsible for executing them may be placed on record in an inheritance document, such as conventional will, a codicil or similar. However, they may also take the form of a specific digital will document that must be recorded in the Electronic Digital Wills Register, dealt with below.

The digital will document can be amended or revoked at any time. To make the system established as secure as possible, it will be invalid if the testator has duly placed on record any other last wishes. This is to avoid any inconsistencies or discrepancies between the content of the last digital wishes included in a will or other similar document and those placed on record in the digital will document recorded in the Electronic Digital Wills Register. As we shall see below, the Digital Wills Act states that no access shall be granted to the Register when other last wishes have been duly placed on record.

If no digital will has been made, the successor or executor may carry out the actions contemplated (notifying the service providers of the death, request for cancellation of the account and request for execution of established contractual clauses or policies, etc.) pursuant to the agreements entered into with the digital service providers.

As noted above, those placing their last digital wishes on record in a digital will document must record it in the Electronic Digital Wills Register. It is important to stress once again that this document shall not be enforceable if other last wishes have been duly placed on record.

Access to the Electronic Digital Wills Register is restricted to the testator of the digital will and, after his or her death, those persons demonstrating a legitimate interest. If it becomes aware of the death of a digital will testator, the Electronic Digital Wills Register may contact the appointed executors on an ex-officio basis. To be able to access this Register, one needs to prove by means of a certificate from the Registry

---

55 The Digital Wills Act also amends Book Two of Catalonia’s Civil Code to contemplate the option of including in the powers, in case of the unexpected loss of capacity over digital wills, the person responsible for executing them and the scope of their management powers. The Act also states that the parents and guardians of minors must ensure that the presence of the latter in digital environments is appropriate and does not create risks for them and, if necessary, that they may take the appropriate measures and seek the assistance of the public authorities.

56 Article 411-10.1 Catalan Civil Code.
57 Article 411-10.2 Catalan Civil Code.
58 Article 411-10.6 Catalan Civil Code.
59 Article 411-10.7 Catalan Civil Code.
60 Article 411-10.1 Catalan Civil Code.
61 Article 421-24.2 Catalan Civil Code.
62 Article 421-2 Catalan Civil Code.
63 Article 411-10.3 Catalan Civil Code.
64 Article 411-10.4 Catalan Civil Code.
65 Article 411-10.5 Catalan Civil Code.
66 Additional Provision Three, Catalan Civil Code. During the peer-review process of this paper, the regulation of the Electronic Digital Wills Register has been appealed by the Spanish Government before the Spanish Constitutional Court (unconstitutionality appeal 4751-2017). As a consequence, the validity and the application of the regulation have been suspended (Art.161.2 Spanish Constitution).
67 Additional Provision Three, Catalan Civil Code.
of Last Wills and Testaments that the testator has not duly placed on record other last wishes.  

The Electronic Digital Will Register may issue, at the request of a digital will executor, a certificate as to the existence or otherwise of a registered digital will document. If the testator does not provide otherwise, this certificate may also identify the persons appointed as digital will executors.

This new legislation has been welcomed by legal doctrine, as can be seen by the statement by Ruda that “although the draft bill cannot resolve all the problems that will be raised in practice, it does seem to resolve some of the most urgent ones, and the global or overall assessment can be positive” (Ruda González, 2017).

5. Some concluding thoughts: criteria for regulating the digital footprint

The development of the information society is becoming ever clearer in many aspects of our lives, but it is also having a greater impact upon our death (Walter et al., 2012). Our presence on the Net leaves a footprint that is manifested in different forms over our lives and is one that must be managed properly when we die.

The mechanisms contemplated by current legislation to manage our footprint in the physical world are not sufficiently up to the task, or make extremely complex, the process of managing our footprint on the Web when we die (Hopkins, 2013). What’s more, these mechanisms have not been updated in response to the new challenges created by the information society (Carroll & Romano, 2010). This gives rise to many different kinds of issues, be they legal, financial or emotional, which will surely only increase as digital natives edge closer to death and their digital footprints continue to expand (Lastowka, 2010; Sy, 2016; Varnado, 2019).

Over the course of the preceding pages, we have had the opportunity to analyze how mechanisms have begun to be implemented to manage the digital footprint of deceased users, on the part of both digital service providers and the different forms of legislation that have been adopted, incipiently, in recent years.

In view of the different initiatives analysed, and the experience gained in their implementation, set out below, by way of conclusion, are some criteria that should guide the regulation of the digital footprint in the case of death.

5.1. Legal certainty

Firstly, any mechanism adopted to manage the digital footprint of digital service users must guarantee legal certainty.

To ensure that this is the case, any mechanisms adopted must allow for the proper understanding of the wishes of the user with regard to the management of their digital footprint upon their death. The user must be able to place on record which digital records making up their digital footprint are to be managed, what steps must be taken with regard to them (ranging from deletion to access or copying) and who should take these steps. In this regard, it should be noted that managing a digital footprint does not necessarily mean that, upon a user’s death, their entire digital footprint can be disclosed to their successors or family members. Although the deceased is not, strictly speaking, the holder of a right to privacy, this should not prove an obstacle to a digital services user deciding, a priori, that a part of their digital footprint can never be disclosed.

The user’s wishes can be placed on record using the mechanisms of inheritance law, such as wills or codicils. However, these mechanisms are not suited to the habits of digital natives or are ruled out by digital service users because they do not have resources that aid them in planning how to manage their estate when they die. That is why there is a need to establish other mechanisms for users to place on record how they wish their digital footprint to be managed when they die, such as the creation of public registers containing documents covering one’s digital will or the accreditation of private companies responsible for documenting these wishes.

At the same time, digital service providers must be sure of the service user’s wishes. If these wishes are placed on record by means of the channels offered by the provider itself, they may require the same identification and authentication methods employed by the user to access the service. If the wishes are expressed using different channels (such as a conventional or digital will), the necessary guarantees need be provided. The wishes expressed by the user cannot be altered (e.g. by furnishing a copy of the will, of certification of the digital will document by the public registry in which it is recorded or by accreditation of the company with which the user has recorded his or her wishes). This certainty must embrace the identity of the person charged with executing the digital will of the deceased user and the scope of their powers.

The users will must be compatible with any agreements he or she has entered into with the digital service providers. Nevertheless, we should be aware of the fact that, in granting their consent, users are often unaware of the implications that this entails, and of what the impact may be with regard to their digital footprint when they are dead. We should also be aware that digital service provider agreements and policies might attach more importance to their own interests than those of their users. In this regard, we need to ensure that agreements on digital services and providers’ policies allow users to decide what should be done with their digital footprint when they die and regard as null any clauses to the contrary.

Furthermore, the user’s wishes have to be compatible with the third-party rights with regard to the data making up the former’s digital footprint. In this regard, it is important to realize that one’s digital footprint can comprise personal data, images or works over which third parties may have some kind of entitlement. Indeed, one should be aware that this is one of the reasons often given by digital service providers to refuse access to a deceased user’s digital footprint. Whatever mechanism is adopted will have to respect the substantive norms governing these matters.

Lastly, whatever mechanism is adopted to manage digital service users’ digital footprint must be aware that users may not have placed their wishes on record. This absence should not be regarded solely as refusing to allow their successors, family members or friends to manage their digital footprint.

68 Additional Provision Three, Catalan Civil Code.
69 Additional Provision Three, Catalan Civil Code.
However, it should limit the scope of the powers of those in charge of managing the digital footprint, for example to deleting the accounts but not accessing their content.

5.2. Effectiveness

Secondly, any mechanism adopted to manage the digital footprint of digital services users must be effective.

The mechanism adopted must permit timely digital footprint management. The death of a family member or friend has a great emotional impact on their surrounding environment, meaning that the digital footprint must be managed expeditiously. Additionally, we need to avoid situations in which digital services cause more suffering for these family members and friends, preventing (for example) a deceased user’s account from continuing to interact with other users.

The mechanism adopted must be assumable by digital service providers (Kutler, 2011). As previously noted, many providers currently base their business model on analysis of the data generated by digital service users, so once the latter have died, they are no longer of interest to the former, even if they are of continued (or even increased) interest to the successors, family and friends of the deceased user. It has been said that regulation of the digital footprint could be educational in nature for both users and providers of digital services (Ruda González, 2017). Nevertheless, we believe that lawmakers should be more ambitious and contribute to the building of new rules of the game that provide a response to the changing conditions encountered after one’s death.

Whatever mechanism is promoted needs to be easily adaptable to any changes in digital services due to developments in technology or social usage thereof. Over the course of their lives, people sign up for dozens if not hundreds of digital services. In addition, over time, they forget which digital services or passwords they have used and the footprint they have generated.

Additionally, any mechanism adopted must, as stated above, initially avoid any “judicialisation” of the management of the deceased’s digital footprint. Obviously, a court judgment on what must be done with a digital footprint is a mechanism with a guarantee and one that provides legal certainty. Nevertheless, it can often be disproportionate when seeking the cancellation of a digital service account or even access to digital records held with a digital service provider, if the user has expressly stated previously that this is their wish. To ensure the greatest possible effectiveness, the courts should be reserved for disputes in which a complex conflict between different rights has been identified, but not for the normal management of the digital footprint.

5.3. Transparency

Thirdly, any mechanism adopted to manage the digital footprint of digital service users must be transparent.

There is a need to guarantee that digital service providers properly notify their users of the policies on digital footprint management. There is also the need to ensure that those charged with managing a digital footprint are made sufficiently aware of the scope of their duties.

Lastly, those charged with managing a digital footprint should be informed of those digital service providers with which the deceased user had entered into some kind of agreement.

As Massimi and Charise (2009) note, information and communication technologies “are not yet designed to effectively acknowledge—or engage with—the inevitable death of their users. Anyway, as far as we are aware, the self-regulation championed by some digital service providers provides a response to numerous demands by both users and their successors or family members after their death. Nevertheless, situations may also arise that limit the ability to act on the part of successors, family members and friends of deceased users (Ruda González, 2017). This is why consideration should be given as to whether it is worth providing regulatory mechanisms for the management of the digital footprint of digital service users after their death.

The aforementioned criteria must allow for the adoption or regulation of mechanisms for managing the digital footprint of digital service user to be clear and trustworthy, efficient and easily recognized and adopted by digital service providers. They must also acknowledge the wishes expressed by the user and the person(s) charged with their management and provide, in all cases, sufficient legal certainty to allow a digital services user an eternal rest in the online world.

Acknowledgement

The author would like to thank Dr. Miquel Peguera for reading this article, and for his comments and suggestions. I am also thankful to Dr. Xavier Bernad for his useful insights. Any errors or inaccuracies it may contain are the exclusive responsibility of the author.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2018.04.008.

REFERENCES


Carroll E, Romano J. Your digital afterlife: when facebook, flickr and twitter are your estate, what’s your legacy?. Berkeley: New Riders; 2010.


Towards visibility: digital assets when death.

Abstract

Digital assets, also known as virtual property, are assets that are stored in digital form. They can include items such as photos, videos, emails, and online accounts. After death, these assets may be subject to various legal issues, including probate, intestacy, and privacy. This article explores the legal issues surrounding digital assets when death and the implications of these issues for post-mortem privacy and the potential for digital assets to be accessed after the death of the owner.

Keywords: digital assets, post-mortem privacy, privacy, afterlife, death.

1. Introduction

The digital age has brought with it a new set of challenges, particularly in the area of digital assets. With the increasing use of digital platforms and the ability to store information in a digital format, there is a growing need for laws and regulations to govern the use and handling of these assets after death.

2. Digital Assets

Digital assets are assets that are stored in digital form. They can include items such as photos, videos, emails, and online accounts. These assets are often stored on platforms such as Facebook, Twitter, and Instagram, and can be accessed through user names and passwords.

3. Legal Issues

After death, digital assets may be subject to various legal issues, including probate, intestacy, and privacy. Probate is the legal process of validating a will or intestacy, which is the legal process that occurs when there is no will. Intestacy is the legal process that occurs when there is no will.

4. Post-Mortem Privacy

Post-mortem privacy is the right of an individual to have control over their digital assets after death. It is an important issue because it involves the potential for digital assets to be accessed after the death of the owner.

5. Conclusion

In conclusion, digital assets are an important issue that requires careful consideration. The legal issues surrounding digital assets when death are complex, and there is a need for laws and regulations to govern the use and handling of these assets after death.

References


Nelson SD, Simek JW. Technology: when you die, will your digital assets go to hell. Res Gestae Indiana Bar J 2016;60.


universitat oberta de catalunya, 2017.

Sherry K. What happens to our facebook accounts when we die?: probate versus policy and the fate of social-media assets postmortem. Pepperdine Law Rev 2013;40(1).


Subotnik EE. Copyright and the living dead?: succession law and the postmortem term. Harv J Law Technol 2015;29(1).

Sy E. The revised uniform fiduciary access to digital assets act: has the law caught up with technology. Touro Law Rev 2016;32(3).

Varnado SS. Your digital footprint left behind at death: an illustration of technology leaving the law behind. Louisiana Law Rev 2014;74(3).


Watkins AF. Digital properties and death: what will your heirs have access to after you die. Buffalo Law Rev 2014;62.

Wright N. Death and the internet: the implications of the digital afterlife. First Monday 2014;6(2).