

## Citation for published version

Cerrillo-i-Martínez, A. (2018). How do we provide the digital footprint with eternal rest? Some criteria for legislation regulating digital wills. *Computer Law and Security Review*, 34(5), 1119-1130. doi: 10.1016/j.clsr.2018.04.008

## 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](mailto:repositori@uoc.edu)





ELSEVIER

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

journal homepage: [www.elsevier.com/locate/CLSR](http://www.elsevier.com/locate/CLSR)


---



---

**Computer Law  
&  
Security Review**


---



---

# 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 Agustrillo-i-Martiz. Published by Elsevier Ltd. All rights reserved.

## 1. The digital footprint<sup>1</sup>

1 A person's digital footprint is made up of all the records that  
2 are in the cloud. They are created when they communicate  
3 with others on the Internet via email, when they take part  
4 in social networks, when they store things, when they share  
5 photos or videos, or when they read books, listen to music,  
6 watch films, play games or make purchases from online stores  
7 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).<sup>2</sup>

The content of the files making up the digital footprint  
differ in nature and value. Some of these records may con-  
tain data protected by different rights, some of them funda-  
mental, such as freedom of expression, secrecy of correspon-  
dence, 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. docu-  
ments or photos). Furthermore, both of these types of records

\* Correspondence to: Law and Political Science Department, Universitat Oberta de Catalunya, Av. Carl Friedrich Gauss, 5, Barcelona 08860, Castelldefels, Spain.

E-mail address: [acerrillo@uoc.edu](mailto:acerrillo@uoc.edu)

<sup>1</sup> 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).

<sup>2</sup> 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).

18 may have an economic value, to a greater or lesser degree  
19 (i.e. bitcoins or money earned on an online gaming site). Oth-  
20 ers, meanwhile, may be—only or additionally—of sentimental  
21 value to the user or their personal or family circle (i.e. cor-  
22 respondence carried out by email, photos shared on family  
23 albums uploaded onto the web or playlists or reading lists  
24 shared with him or her). Some, such as emails, may even be of  
25 value greater to that inherent in them, as master keys that al-  
26 low users to manage their digital footprint in digital services,  
27 in saving the data necessary to access them (Carroll & Ro-  
28 mano, 2010, 109).

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

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

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

39 It is not just that. When a user dies, their successors, rela-  
40 tions and friends often find it impossible or difficult to manage  
41 the files making up the former's digital footprint, whether in  
42 terms of deleting it, accessing it or keeping it alive.

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

46 For example, one might recall the case of the parents of a  
47 soldier killed in Iraq who wished to access the emails sent by  
48 their son from the front, to create a memorial to him, which  
49 Yahoo refused until access was granted by a judge (Lastowka,  
50 2010).<sup>3</sup> There is also the tale of a Virginia family who sought,  
51 in vain, to access the Facebook profile of their son, who had  
52 committed suicide at the age of 15, to investigate the circum-  
53 stances that had led to his death (Varnado, 2014; Watkins,  
54 2014).

55 These and other issues that have arisen over recent years  
56 have led some digital service providers, although initially re-  
57 luctant to do so, to make changes to their policies to provide a  
58 response to this new reality. The social pressure often accom-  
59 panying these lawsuits has meant that different rulings have  
60 begun to adopt some legislation with mechanisms enabling  
61 management of a deceased user's digital footprint. It is easy  
62 to appreciate how, as McCallig points out, "a bereaved family  
63 in dispute with Facebook often makes a national or interna-  
64 tional news story" (McCallig, 2014).

65 Digital service providers have no incentive *a priori* to do  
66 anything with regard to managing the digital footprint of dead  
67 users, in that they generally base their business model, the  
68 free-of-charge nature of their services, on the use they make of  
69 the information generated by their living users' activities. This  
70 is why doing anything with regard to deceased users' digital  
71 footprints would normally entail spending time and money  
72 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 prefer-  
ences in this regard. Additionally, recent years have seen the  
appearance of companies offering to manage the digital ser-  
vice 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 foot-  
prints when users die (Edwards & Harbinja, 2013). Therefore,  
to provide a global and comprehensive response to the differ-  
ent 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 foot-  
print management is still not a generalized social concern, de-  
spite the stories appearing in the media.<sup>4</sup> Indeed, a US survey  
shows how 63% of Americans make no plans for their digi-  
tal footprint after their death.<sup>5</sup> 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.<sup>6</sup>

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 digi-  
tal services or new social uses of information and communi-  
cation technologies (McCarthy, 2015). Indeed, the problem has  
only just begun and digital footprint management will surely

<sup>4</sup> For example, "Como preparar la muerte digital" (2015),  
El Mundo <http://www.elmundo.es/tecnologia/2015/10/31/5633c0c2ca4741bb188b461a.html>; "La muerte toca lo digi-  
tal" (2015), ABC <http://www.abc.es/tecnologia/redes/20150221/abci-facebook-redes-cibermuerte-201502182107.html>;  
"Dret a la mort digital" (2016), La Vanguardia (29/02/2016)  
<http://www.lavanguardia.com/vida/20160229/4085404087/dret-a-la-mort-digital.html>. "Bequeathing the keys  
to your digital afterlife" (2013), New York Times  
<http://www.nytimes.com/2013/05/26/technology/estate-planning-is-important-for-your-online-assets-too.html>;  
"End of life tech companies grow with changes in death traditions"  
(2013), Huffington Post, [http://www.huffingtonpost.com/2013/06/13/end-of-life-death-tech-funeral\\_n\\_3431174.html](http://www.huffingtonpost.com/2013/06/13/end-of-life-death-tech-funeral_n_3431174.html); "Death on  
Facebook now common as 'dead profiles' create vast virtual  
cemetery" (2012), Huffington Post [http://www.huffingtonpost.com/2012/12/07/death-facebook-dead-profiles\\_n\\_2245397.html](http://www.huffingtonpost.com/2012/12/07/death-facebook-dead-profiles_n_2245397.html);  
Cyberspace when you're dead (2011), New York Times <http://www.nytimes.com/2011/01/09/magazine/09Immortality-t.html>  
(last consulted September 2017).

<sup>5</sup> <http://www.nextavenue.org/5-steps-creating-your-digital-estate-plan/>; "Leaving Behind the Digital Keys to Financial Lives"  
(2013), New York Times [http://www.nytimes.com/2013/05/25/your-money/forgotten-in-estate-planning-online-passwords.html?nl=todaysheadlines&emc=edit\\_th\\_20130525&r=2&](http://www.nytimes.com/2013/05/25/your-money/forgotten-in-estate-planning-online-passwords.html?nl=todaysheadlines&emc=edit_th_20130525&r=2&) (last  
consulted September 2017).

<sup>6</sup> Nevertheless, there are almost no studies on soci-  
etal concern on the digital estate and on how it should  
be administered after a person dies or is incapacitated.  
We are only aware of one: "La muerte toca lo digital"  
(2015), ABC <http://www.abc.es/tecnologia/redes/20150221/abci-facebook-redes-cibermuerte-201502182107.html>.

<sup>3</sup> Who owns your e-mails? BBC News [http://news.bbc.co.uk/2/hi/uk\\_news/magazine/4164669.stm](http://news.bbc.co.uk/2/hi/uk_news/magazine/4164669.stm) (last consulted August 2017).

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

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

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

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

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

## 2. Digital footprint management initiatives

126 The majority of a digital footprint is controlled by digital ser-  
127 vice providers via their terms of service agreements, and the  
128 policies governing the provision of most digital services gen-  
129 erally establish the use that can be made of the records cre-  
130 ated by the activities carried on by users (Edwards & Harbinja,  
131 2013).

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

138 As a starting point, one might highlight the fact that, in  
139 most cases, agreements with digital service providers do not  
140 establish maximum terms of enforceability, nor do they in-  
141 clude clauses on the impact that the user's death may have  
142 upon the agreement.<sup>8</sup> However, some providers do indeed ex-  
143 plicitly contemplate in their agreements that the user's death  
144 implies termination thereof (with the so-called "No Right of  
145 Survivorship" clauses) (Watkins, 2014).<sup>9</sup>

<sup>7</sup> 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/life-style/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).

<sup>8</sup> 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}.

<sup>9</sup> For example, in the case of Apple: <http://www.apple.com/legal/icloud/en/terms.html> and Yahoo <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html> (last consulted August 2017).

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

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

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

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

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

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

### 2.1. Leading digital service providers' policies on deceased user accounts

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

<sup>10</sup> 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 at: <https://es-es.facebook.com/legal/terms/update> (last consulted August 2017).

<sup>11</sup> Catalonia's Civil Code states that a person's "civil personality" is extinguished with their death (Art. 211-1).

<sup>12</sup> "Average Person Uses 10 Online Passwords a Day" (2011). *The Telegraph* <http://www.telegraph.co.uk/technology/news/8602346/Average-person-uses-10-online-passwords-a-day.html> (last consulted September 2017).

<sup>13</sup> 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).



189 agreements to include mechanisms for managing digital foot- 242  
190 prints after a user's death. 243

191 It should be emphasized that these are often agreements 244  
192 for which consent is provided by clicking on a box (*clickwrap* 245  
193 *agreements*) or by scrolling down the agreement (*browse-wrap* 246  
194 *agreements*), whose users do not generally read their contents 247  
195 (*Fernández Flores, 2015*). Above and beyond their acceptance 248  
196 as an effective mechanism for placing on record user consent 249  
197 (*Dickens, 2007*), it is clear that, from the standpoint of this ar- 250  
198 ticle, users are unaware of the impact all this has on the man- 251  
199 agement of their footprint after their death. 252

200 The impact of digital footprint management goes beyond 253  
201 the securing of the cancellation of accounts or access to 254  
202 records. In recent years, we have witnessed how the manage- 255  
203 ment of the deceased's digital footprint may also have sig- 256  
204 nificant effect on the grieving process of family and friends 257  
205 shared over the Web and, in general, on the process of pub- 258  
206 lication of the death (*Wright, 2014; Bassett, 2015; Sofkaet al.,* 259  
207 *2012*). 260

208 Set out below is a brief summary of some providers' poli- 261  
209 cies in this regard. 262

#### 210 2.1.1. Facebook 263

211 To begin with, it should be noted that Facebook's Statement 264  
212 of Rights and Responsibilities grants no third-party beneficial 265  
213 interests.<sup>14</sup> What's more, it states that users accept the un- 266  
214 dertaking not to share their passwords or let anyone else ac- 267  
215 cess their account.<sup>15</sup> Furthermore, it contains no provision ex- 268  
216 pressly establishing that the agreement with the user termi- 269  
217 nates upon the latter's death (*McCallig, 2014*). 270

218 Nevertheless, Facebook now offers the option that, when 271  
219 a user dies, their accounts be "memorialized" or definitively 272  
220 deleted at the proposal of a successor or family member 273  
221 (*Sherry, 2013*). 274

222 The social media network's policy on digital footprint man- 275  
223 agement has evolved since its appearance, as users have de- 276  
224 manded that the company offer the option that friendships 277  
225 be linked with content created by the deceased (*McCallig,* 278  
226 *2014*). Indeed, after a campaign by friends of the Virginia Tech 279  
227 mass shooting of April 2007, Facebook amended its initial pol- 280  
228 icy of deleting accounts of deceased users after thirty days, 281  
229 adding the possibility of converting the account into a memo- 282  
230 rial (*Mazzone, 2011; McCallig, 2014; Bassett, 2015*). Over the 283  
231 course of time, the possibility of creating this "memorialized" 284  
232 page seems to be the most popular option, particularly with 285  
233 active Web users, such as the young, or users who have died 286  
234 under violent circumstances (*Leaver, 2013*). 287

235 With the memorialized account, the user's friends can con- 288  
236 tinue to post to the former's page as they had been doing when 289  
237 he or she was still alive, thus turning Facebook into a space 290  
238 for managing grief and pain. The wall's content will be just as 291  
239 accessible as before, allowing Facebook friends to post mes- 292  
240 sages and photos and, ultimately, share their grief (*McEwen &* 293  
241 *Scheaffer, 2013*). 294

The memorialized account is administered by a "legacy 242  
contact" chosen by the user.<sup>16</sup> This legacy contact has very 243  
limited administration powers over the account, such as 244  
adding a pinned post to the memorialized profile (e.g. a last 245  
message on behalf of the deceased user), responding to new 246  
friend requests and updating the deceased users' profile pic- 247  
ture and cover photo. However, they cannot enter into the ac- 248  
count as if they were the user, nor delete or modify anything 249  
posted by the user, nor remove people from their friend list. 250

Facebook provides the option of the account owner giving 251  
the legacy contact permission to download a copy of what 252  
they have published on their account (such as photos, videos, 253  
profile information, events and friends lists). However, it does 254  
not provide access to other content, such as messages or ad- 255  
verts they may have accessed, unless so provided for in a 256  
will or other valid consent document that contains express 257  
authorisation.<sup>17</sup> 258

Removal of the account is contemplated for those cases in 259  
which the user has so stated a preference in the space de- 260  
signed for the purpose. Facebook also accepts requests for 261  
removal from close family members or executors, provided 262  
they can provide proof of authority and a document placing 263  
the death on record (death certificate, obituary or memorial 264  
card).<sup>18</sup> 265

#### 266 2.1.2. Google 267

Google's policy is based on providing account holders with an 268  
"inactive account manager".<sup>19</sup> 269

Using this inactive account manager, users can tell Google 270  
what to do after their account has been inactive for a certain 271  
period.<sup>20</sup> The inactive account manager allows them to spec- 272  
ify how long the account shall remain unused before being 273  
regarded as inactive. It also allows them to provide a mobile 274  
phone number or an email address that Google will contact 275  
before taking any action. Lastly, it allows them to choose up to 276  
ten friends or trusted contacts that Google will notify that the 277  
account is inactive. 278

Google users can specify that their data be shared with 279  
these trusted contacts. They can also indicate that any mes- 280  
sages sent to the inactive account receive an automatic reply. 281  
Lastly, they can tell Google to delete the account when it be- 282  
comes inactive. 283

Google also allows people to request access to an account 284  
or that a deceased user's account be deleted. However, in such 285  
a case, Google will review the request and take a decision. This 286  
decision will be made, according to Google, taking into account 287  
its responsibility to keep people's information safe, secure and 288

<sup>16</sup> <https://www.facebook.com/help/103897939701143> (last consulted August 2017).

<sup>17</sup> <https://www.facebook.com/help/408044339354739> (last consulted August 2017).

<sup>18</sup> <https://es-es.facebook.com/help/1518259735093203?ref=related> (last consulted August 2017).

<sup>19</sup> <https://myaccount.google.com/inactive> (last consulted August 2017).

<sup>20</sup> <https://support.google.com/accounts/answer/3036546> (last consulted August 2017).

<sup>14</sup> <https://www.facebook.com/legal/terms> (last consulted August 2017).

<sup>15</sup> <https://es-es.facebook.com/legal/terms/update> (last consulted August 2017).

288 private, meaning it cannot, for example, provide passwords or  
289 other login details.<sup>21</sup>

290 Lastly, Google has also established a specific procedure for  
291 requesting reimbursement of deceased user funds in Google's  
292 possession (income from the AdSense program or Google on-  
293 line payment service balances).<sup>22</sup>

### 294 2.1.3. Instagram

295 Instagram has a policy similar to Facebook's, allowing a de-  
296 ceased user's immediate family members to notify it of a  
297 user's death and either memorializing or removing the ac-  
298 count.<sup>23</sup>

299 To memorialize the account, all that is needed is for anyone  
300 to provide Instagram with proof of death, such as an obituary  
301 or news article.

302 To remove the account, an immediate family member must  
303 provide notice and submit the deceased person's birth certifi-  
304 cate, death certificate or proof of authority as legal represen-  
305 tative or his/her successor.<sup>24</sup>

### 306 2.1.4. Twitter

307 Twitter provides a form for a deceased user's representative  
308 or direct family member to request removal of the account.<sup>25</sup>  
309 The applicant must provide proof of the user's death. Under  
310 no circumstances can access to the deceased user's account  
311 be provided.

312 Twitter also offers immediate family members and other  
313 authorized individuals the possibility of removing certain im-  
314 agery via a form for removing images or videos belonging to  
315 the deceased user. Before removing the information, Twitter  
316 will consider its public interest and newsworthiness.<sup>26</sup>

### 317 2.1.5. LinkedIn

318 LinkedIn allows anyone who becomes aware of the passing  
319 of a community member to provide notice of the fact for the  
320 account to be closed and his or her profile to be removed.<sup>27</sup>

321 To do this, they need to fill in a form with the deceased  
322 member's name, the URL of their LinkedIn profile, their rela-  
323 tionship to the deceased, the date of their passing, a link to the  
324 obituary and the company they most recently worked at.<sup>28</sup>

<sup>21</sup> <https://support.google.com/accounts/troubleshooter/6357590?hl=es&rd=2> (last consulted August 2017).

<sup>22</sup> <https://support.google.com/accounts/troubleshooter/6357590?hl=es&rd=2> (last consulted August 2017).

<sup>23</sup> <https://es-la.facebook.com/help/instagram/264154560391256> (last consulted August 2017).

<sup>24</sup> [https://help.instagram.com/contact/1474899482730688?helpref=faq\\_content](https://help.instagram.com/contact/1474899482730688?helpref=faq_content) (last consulted August 2017).

<sup>25</sup> <https://support.twitter.com/articles/20169203> (last consulted August 2017).

<sup>26</sup> <https://support.twitter.com/articles/20174904> (last consulted August 2017).

<sup>27</sup> <https://www.linkedin.com/help/linkedin/answer/6107> (last consulted August 2017).

<sup>28</sup> <https://www.linkedin.com/help/linkedin/ask/ts-rdmlp> (last consulted August 2017).

### 2.1.6. Dropbox

Dropbox has established a procedure to request access to a de-  
ceased user's account.<sup>29</sup> To be able to access the account, the  
applicant must provide by conventional post a valid court or-  
der 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

Alongside the 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.<sup>30</sup>

Firstly, there are companies that help people decide what is  
to be done with their digital footprint. These companies im-  
properly 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.<sup>31</sup>

Secondly, there are companies that delete the digital foot-  
print, managing the cancellation of accounts and wiping the  
deceased person's presence from the Internet.<sup>32</sup>

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.<sup>33</sup>  
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 de-  
ceased.<sup>34</sup>

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 insur-  
ance company removing the insured's profiles from all social  
media networks, and deleting their blogs and email accounts.

<sup>29</sup> <https://www.dropbox.com/es/help/security/access-account-of-someone-who-passed-away> (last consulted August 2017).

<sup>30</sup> Basset refers to two categories of companies: asset maintenance and posthumous scheduling (Basset, 2015).

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

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

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

<sup>34</sup> See, for example, Eternime (<http://eterni.me/>) or Lifonaut (<https://www.lifonaut.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; Marwick & 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



482 agreements signed with digital service providers or with their  
483 terms of service.

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

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

### 498 3.1. Regulating the digital footprint as an asset: the case 499 of the *United States of America*

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

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

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

521 One the one hand, the Uniform Fiduciary Access to Digital  
522 Assets Act (UFADAA), promoted by the National Conference of  
523 Commissioners on Uniform State Laws, of which two versions  
524 are available (2014 and 2015),<sup>35</sup> has been or is in the process of  
525 being adopted by 24 states.<sup>36</sup>

526 According to the UFADAA, digital assets are electronic  
527 records in which individuals have a right or interest.<sup>37</sup> The  
528 UFADAA seeks, firstly, to give fiduciaries the legal authority to  
529 manage digital assets and electronic communications in the  
530 same way they manage tangible assets and financial accounts.  
531 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,  
it provides that the digital “custodians” must provide digital  
tools to permit users to decide whether they wish to disclose  
some or all of the records making up their digital footprint.<sup>38</sup>  
So, if the custodian provides an online tool (separate from the  
terms of service agreement), the user's direction, as expressed  
via this tool, is legally enforceable. If an online tool is not pro-  
vided to express the user's direction, or if the latter does not  
use it, the user may give binding instructions in a will, trust,  
power of attorney or other written record.<sup>39</sup> The directions so  
provided by the user override any terms of service agreement  
signed with the digital service provider.<sup>40</sup>

When disclosing digital assets, the custodian may choose  
whether to grant full or partial access, or whether to provide a  
copy of the files.<sup>41</sup> The custodian may decide upon a charge for  
disclosing the digital assets.<sup>42</sup> If something is requested that  
represents an undue burden, the custodian can refuse to pro-  
vide access and a court order will be required to be able to gain  
access.<sup>43</sup> The UFADAA establishes the different procedures to  
be followed by different parties to access the digital assets.

Alternatively, there is the Privacy Expectation Afterlife and  
Choices Act (PEAC), promoted by NetChoice.<sup>44</sup> According to  
this model, providers only need provide access pursuant to a  
court order.<sup>45</sup> What's more, this model establishes very strict  
conditions for the court to authorize access: that the user is  
proven dead; that the user is a subscriber or customer; that  
the account has been identified specifically and that there are  
no other authorized users or owners of the account; that the  
request for disclosure is tailored narrowly to effect the pur-  
pose of the administration of the estate; that the executor or  
administrator demonstrates a good faith belief that account  
records are relevant to resolve fiscal aspects of the estate; that  
the request seeks information spanning no more than a year  
prior to the date of death; and that the request is not in conflict  
with the deceased user's will or testament. It also establishes  
that providers cannot be compelled to disclose any records  
under certain circumstances, for example, when the deceased  
user has expressed a different intent through deletion of the  
records or by indicating to the provider itself how they were  
to be dealt with.<sup>46</sup> Lastly, it states that a provider shall not be  
required to allow anyone to assume control of the deceased  
user's account.<sup>47</sup>

<sup>38</sup> Section 4 (a).

<sup>39</sup> Section 4 (b).

<sup>40</sup> Section 4 (c).

<sup>41</sup> Section 6 (a).

<sup>42</sup> Section 6 (b).

<sup>43</sup> Section 6 (d).

<sup>44</sup> Accessible at: <https://netchoice.org/library/privacy-expectation-afterlife-choices-act-peac/> (last consulted August 2017).

<sup>45</sup> Section 1(a).

<sup>46</sup> Section 3.

<sup>47</sup> Section 5.

<sup>35</sup> The latter version of the Revised UFADAA has been welcomed by legal doctrine (Nelson & Simek, 2016).

<sup>36</sup> Accessible at: [http://www.uniformlaws.org/shared/docs/Fiduciary\\_Access\\_to\\_Digital\\_Assets/2015\\_RUFADAA\\_Final\\_Act\\_2016mar8.pdf](http://www.uniformlaws.org/shared/docs/Fiduciary_Access_to_Digital_Assets/2015_RUFADAA_Final_Act_2016mar8.pdf) (last consulted August 2017).

<sup>37</sup> Section 2 (10).



578 In addition to the legislation adopted, one cannot ignore  
579 the role played by the courts with regard to digital footprint  
580 management (Watkins, 2014).

### 581 3.2. *Regulating the digital footprint as protection of the* 582 *deceased's data: the case of France*

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

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

591 The Digital Republic Act contains provisions on the man-  
592 agement of deceased persons' personal data.<sup>48</sup> To begin with,  
593 it recognizes that people's rights with regard to the processing  
594 of personal data expire with the death of their owner. Never-  
595 theless, they may remain provisionally in force for managing  
596 their digital footprint.<sup>49</sup> In this regard, it contemplates the op-  
597 tion of arranging during one's lifetime the conditions for con-  
598 serving and communicating personal data after one's death.

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

607 Firstly, the option is contemplated of adopting general in-  
608 structions on the person's personal data as a whole. These in-  
609 structions can be registered with "digitally trusted" third par-  
610 ties certified by the country's National Commission for Infor-  
611 mation Technology and Civil Liberties (CNIL).<sup>50</sup>

612 Secondly, there are specific instructions on the processing  
613 of personal data. These instructions are aimed at data con-  
614 trollers. They are subject to the express consent of the inter-  
615 ested party and cannot arise solely from their acceptance of  
616 the general terms of service.<sup>51</sup>

617 In their instructions, users can appoint a person responsi-  
618 ble for executing them. When this person becomes aware of  
619 the user's passing, he or she can discover the content of the  
620 instructions and request that the data controllers implement  
621 them. If no such person is appointed or, unless there is an in-  
622 struction to the contrary, the appointee has also passed away,  
623 the user's successors are entitled to acquaint themselves with  
624 the instructions and request that the data controllers imple-  
625 ment them.

626 Any agreements signed with digital service providers lim-  
627 iting the prerogatives recognized in the Act shall be regarded  
628 as not entered into.<sup>52</sup>

<sup>48</sup> Article 40.1.II.

<sup>49</sup> Article 40.1.I.

<sup>50</sup> Article 40.1.II.

<sup>51</sup> Article 40.1.II.

<sup>52</sup> Article 40.1.II.

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.<sup>53</sup> Additionally, the suc-  
cessors 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.<sup>54</sup>

## 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 Catalo-  
nia, 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 ser-  
vices 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 pow-  
ers 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 en-  
gineers 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, Cat-  
alonia'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

<sup>53</sup> Article 40.1.III.

<sup>54</sup> Article 40.1.IV.

677 power to regulate the digital footprint based on this power, as  
678 France has done.

679 On the other hand, Article 129 of the Statute states that  
680 Catalonia has exclusive powers in the field of civil law. The  
681 provisions of Article 149.1.8 of the Spanish Constitution limit  
682 this power. According to the precedent set by Spain's Consti-  
683 tutional Court, autonomous community powers must be exer-  
684 cised with regard to the "conservation, modification and im-  
685 plementation" that constitute the limit of the attributable and  
686 exercisable powers (Judgment 31/2010). In particular, the Court  
687 had previously held that "the Constitution permits that pre-  
688 existing special or local civil rights may be the object not just  
689 of 'conservation' and 'modification', but also of legislative ac-  
690 tion that enables their organic growth, thereby acknowledging  
691 not only the historical nature and current enforceability, but  
692 also the future vitality of said pre-constitutional regulations".  
693 According to the Court, it "permits the legislative regulation of  
694 fields previously not governed by the Law" (STC 88/1993, FJ 3).

695 Finally, Catalonia has also exclusive powers on administra-  
696 tive **organisation** and mechanisms of public activity (Art.150).

#### 697 4.2. The **Digital Wills Act**

698 The Digital Wills Act amends a number of precepts of Catalo-  
699 nia's Civil Code to acknowledge that people can place their  
700 digital wills on record in the case of their death.<sup>55</sup> Digital wills,  
701 in the case of death, are the provisions established by a person  
702 so that, when they die, their successor or executor, or the per-  
703 son appointed to execute them, may act before those digital  
704 service providers with whom the user has an active account.<sup>56</sup>

705 Digital service users may place on record the content and  
706 the scope of the tasks to be performed. These tasks may  
707 include a range of steps, including notifying digital service  
708 providers of the death of the user, requesting that digital ser-  
709 vice providers cancel active accounts, requesting that digital  
710 service providers execute contractual clauses or activate poli-  
711 cies established in the case of a user's death and, if appli-  
712 cable, that they issue a copy of any digital records on their  
713 servers.<sup>57</sup> It is interesting to note that the Digital Wills Act  
714 contemplates that those responsible for executing the digital  
715 wills may not have access to the contents of the accounts or  
716 the digital records unless the user so establishes in their will  
717 or a court order to the effect is secured.<sup>58</sup> Any costs arising  
718 from the execution of the digital will be borne by the estate,  
719 unless the testator has indicated otherwise.<sup>59</sup>

720 Additionally, digital wills can also appoint the person re-  
721 sponsible for executing them. This person may be either a

successor or any other person named by the testator.<sup>60</sup> The  
appointee can also be a legal person, e.g. a digital estate man-  
agement company. The digital will testator may indicate the  
natural or legal person(s) who are to be informed of the ex-  
istence of the digital will upon the former's death.<sup>61</sup> In the  
absence of any such express appointment, execution of the  
digital will shall fall to the successor, executor or personal rep-  
resentative of the estate, who may execute the digital will or  
appoint another person to execute it.<sup>62</sup> The person responsi-  
ble 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.<sup>63</sup>

The digital will document can be amended or revoked at  
any time. To make the system established as secure as possi-  
ble, it will be invalid if the testator has duly placed on record  
any other last wishes.<sup>64</sup> 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 Elec-  
tronic 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.<sup>65</sup>

As noted above, those placing their last digital wishes on  
record in a digital will document must record it in the Elec-  
tronic Digital Wills Register.<sup>66</sup> 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 be-  
comes aware of the death of a digital will testator, the Elec-  
tronic Digital Wills Register may contact the appointed execu-  
tors on an ex-officio basis.<sup>67</sup> To be able to access this Register,  
one needs to prove by means of a certificate from the Registry

<sup>55</sup> 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.

<sup>56</sup> Article 411-10.1 Catalan Civil Code.

<sup>57</sup> Article 411-10.2 Catalan Civil Code.

<sup>58</sup> Article 411-10.6 Catalan Civil Code.

<sup>59</sup> Article 411-10.7 Catalan Civil Code.

<sup>60</sup> Article 411-10.1 Catalan Civil Code.

<sup>61</sup> Article 421-24.2 Catalan Civil Code.

<sup>62</sup> Article 421-2 Catalan Civil Code.

<sup>63</sup> Article 411-10.3 Catalan Civil Code.

<sup>64</sup> Article 411-10.4 Catalan Civil Code.

<sup>65</sup> Article 411-10.5 Catalan Civil Code.

<sup>66</sup> 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).

<sup>67</sup> Additional Provision Three, Catalan Civil Code.

768 of Last Wills and Testaments that the testator has not duly  
769 placed on record other last wishes.<sup>68</sup>

770 The Electronic Digital Will Register may issue, at the re-  
771 quest of a digital will executor, a certificate as to the existence  
772 or otherwise of a registered digital will document. If the testa-  
773 tor does not provide otherwise, this certificate may also iden-  
774 tify the persons appointed as digital will executors.<sup>69</sup>

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

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

781 The development of the information society is becoming ever  
782 clearer in many aspects of our lives, but it is also having a  
783 greater impact upon our death (Walter et al., 2012). Our pres-  
784 ence on the Net leaves a footprint that is manifested in dif-  
785 ferent forms over our lives and is one that must be managed  
786 properly when we die.

787 The mechanisms contemplated by current legislation to  
788 manage our footprint in the physical world are not sufficiently  
789 up to the task, or make extremely complex, the process of  
790 managing our footprint on the Web when we die (Hopkins,  
791 2013). What’s more, these mechanisms have not been up-  
792 dated in response to the new challenges created by the in-  
793 formation society (Carroll & Romano, 2010). This gives rise to  
794 many different kinds of issues, be they legal, financial or emo-  
795 tional, which will surely only increase as digital natives edge  
796 closer to death and their digital footprints continue to expand  
797 (Lastowka, 2010; Sy, 2016; Varnado, 2014).

798 Over the course of the preceding pages, we have had the  
799 opportunity to analyse how mechanisms have begun to be im-  
800 plemented to manage the digital footprint of deceased users,  
801 on the part of both digital service providers and the different  
802 forms of legislation that have been adopted, incipiently, in re-  
803 cent years.

804 In view of the different initiatives analysed, and the experi-  
805 ence gained in their implementation, set out below, by way of  
806 conclusion, are some criteria that should guide the regulation  
807 of the digital footprint in the case of death.

### 5.1. Legal certainty

809 Firstly, any mechanism adopted to manage the digital foot-  
810 print of digital service users must guarantee legal certainty.

811 To ensure that this is the case, any mechanisms adopted  
812 must allow for the proper understanding of the wishes of the  
813 user with regard to the management of their digital footprint  
814 upon their death. The user must be able to place on record  
815 which digital records making up their digital footprint are to  
816 be managed, what steps must be taken with regard to them  
817 (ranging from deletion to access or copying) and who should

818 take these steps. In this regard, it should be noted that man-  
819 aging a digital footprint does not necessarily mean that, upon  
820 a user’s death, their entire digital footprint can be disclosed to  
821 their successors or family members. Although the deceased  
822 is not, strictly speaking, the holder of a right to privacy, this  
823 should not prove an obstacle to a digital services user decid-  
824 ing, *a priori*, that a part of their digital footprint can never be  
825 disclosed.

826 The user’s wishes can be placed on record using the mech-  
827 anisms of inheritance law, such as wills or codicils. However,  
828 these mechanisms are not suited to the habits of digital na-  
829 tives or are ruled out by digital service users because they do  
830 not have resources that aid them in planning how to man-  
831 age their estate when they die. That is why there is a need to  
832 establish other mechanisms for users to place on record how  
833 they wish their digital footprint to be managed when they die,  
834 such as the creation of public registers containing documents  
835 covering one’s digital will or the accreditation of private com-  
836 panies responsible for documenting these wishes.

837 At the same time, digital service providers must be sure  
838 of the service user’s wishes. If these wishes are placed on  
839 record by means of the channels offered by the provider it-  
840 self, they may require the same identification and authenti-  
841 cation methods employed by the user to access the service. If  
842 the wishes are expressed using different channels (such as a  
843 conventional or digital will), the necessary guarantees need be  
844 provided. The wishes expressed by the user cannot be altered  
845 (e.g. by furnishing a copy of the will, of certification of the digi-  
846 tal will document by the public registry in which it is recorded  
847 or by accreditation of the company with which the user has  
848 recorded his or her wishes). This certainty must embrace the  
849 identity of the person charged with executing the digital will  
850 of the deceased user and the scope of their powers.

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

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

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

<sup>68</sup> Additional Provision Three, Catalan Civil Code.

<sup>69</sup> Additional Provision Three, Catalan Civil Code.



878 However, it should limit the scope of the powers of those in  
879 charge of managing the digital footprint, for example to delet-  
880 ing the accounts but not accessing their content.

### 881 5.2. Effectiveness

882 Secondly, any mechanism adopted to manage the digital foot-  
883 print of digital services users must be effective.

884 The mechanism adopted must permit timely digital foot-  
885 print management. The death of a family member or friend  
886 has a great emotional impact on their surrounding environ-  
887 ment, meaning that the digital footprint must be managed ex-  
888 peditiously. Additionally, we need to avoid situations in which  
889 digital services cause more suffering for these family mem-  
890 bers and friends, preventing (for example) a deceased user's  
891 account from continuing to interact with other users.

892 The mechanism adopted must be assumable by digital  
893 service providers (Kutler, 2011). As previously noted, many  
894 providers currently base their business model on analysis of  
895 the data generated by digital service users, so once the latter  
896 have died, they are no longer of interest to the former, even if  
897 they are of continued (or even increased) interest to the suc-  
898 cessors, family and friends of the deceased user. It has been  
899 said that regulation of the digital footprint could be educa-  
900 tional in nature for both users and providers of digital services  
901 (Ruda González, 2017). Nevertheless, we believe that lawmak-  
902 ers should be more ambitious and contribute to the building of  
903 new rules of the game that provide a response to the changing  
904 conditions encountered after one's death.

905 Whatever mechanism is promoted needs to be easily  
906 adaptable to any changes in digital services due to develop-  
907 ments in technology or social usage thereof. Over the course  
908 of their lives, people sign up for dozens if not hundreds of dig-  
909 ital services. In addition, over time, they forget which digital  
910 services or passwords they have used and the footprint they  
911 have generated.

912 Additionally, any mechanism adopted must, as stated  
913 above, initially avoid any “judicialisation” of the management  
914 of the deceased's digital footprint. Obviously, a court judgment  
915 on what must be done with a digital footprint is a mechanism  
916 with a guarantee and one that provides legal certainty. Nev-  
917 ertheless, it can often be disproportionate when seeking the  
918 cancellation of a digital services account or even access to dig-  
919 ital records held with a digital service provider, if the user has  
920 expressly stated previously that this is their wish. To ensure  
921 the greatest possible effectiveness, the courts should be re-  
922 served for disputes in which a complex conflict between dif-  
923 ferent rights has been identified, but not for the normal man-  
924 agement of the digital footprint.

### 925 5.3. Transparency

926 Thirdly, any mechanism adopted to manage the digital foot-  
927 print of digital service users must be transparent.

928 There is a need to guarantee that digital service providers  
929 properly notify their users of the policies on digital footprint  
930 management.

931 There is also the need to ensure that those charged with  
932 managing a digital footprint are made sufficiently aware of the  
933 scope of their duties.

934 Lastly, those charged with managing a digital footprint 934  
935 should be informed of those digital service providers with 935  
936 which the deceased user had entered into some kind of agree- 936  
937 ment. 937

938 As Massimi and Charise (2009) note, information and com- 938  
939 munication technologies “are not yet designed to effectively 939  
940 acknowledge—or engage with—the inevitable death of their 940  
941 user”. Anyway, as far as we are aware, the self-regulation 941  
942 championed by some digital service providers provides a re- 942  
943 sponse to numerous demands by both users and their succes- 943  
944 sors or family members after their death. Nevertheless, situ- 944  
945 ations may also arise that limit the ability to act on the part 945  
946 of successors, family members and friends of deceased users 946  
947 (Ruda González, 2017). This is why consideration should be 947  
948 given as to whether it is worth providing regulatory mecha- 948  
949 nisms for the management of the digital footprint of digital 949  
950 service users after their death. 950

951 The aforementioned criteria must allow for the adoption 951  
952 or regulation of mechanisms for managing the digital foot- 952  
953 print of digital service user to be clear and trustworthy, ef- 953  
954 ficient and easily recognized and adopted by digital service 954  
955 providers. They must also acknowledge the wishes expressed 955  
956 by the user and the person(s) charged with their management 956  
957 and provide, in all cases, sufficient legal certainty to allow a 957  
958 digital services user an eternal rest in the online world. 958

## Acknowledgement

959 The author would like to thank Dr. Miquel Peguera for read- 959  
960 ing this article, and for his comments and suggestions. I am 960  
961 also thankful to Dr. Xavier Bernadí for his useful insights. Any 961  
962 errors or inaccuracies it may contain are the exclusive respon- 962  
963 sibility of the author. 963

## Supplementary materials

964 Supplementary material associated with this article can be 964  
965 found, in the online version, at doi:10.1016/j.clsr.2018.04.008. 965

## REFERENCES

- Bassett DJ. Who wants to live forever? living, dying and grieving 966  
in our digital society. *Soc Sci* 2015;4(4):1127–39. 967  
doi:10.3390/socsci4041127. 968
- Buitelaar JC. Post-mortem privacy and informational 969  
self-determination. *Ethics Inf Technol* 2017;19(2):129–42. 970  
doi:10.1007/s10676-017-9421-9. 971
- Carroll E, Romano J. Your digital afterlife: when facebook, flickr 972  
and twitter are your estate, what's your legacy?. Berkeley: New 973  
Riders; 2010. 974
- Connor, J. (2010). Digital life after death: the issue of planning for 975  
a person's digital assets after death. Texas Tech School of Law 976  
Legal Studies Research Paper, 02. doi:10.2139/ssrn.1811044. 977
- Desai DR. The life and death of copyright, 11. *Wisconsin Law* 978  
*Review*; 2011. 979
- Dickens RL. Finding common ground in the world of electronic 980  
contracts: the consistency of legal reasoning in clickwrap 981  
cases. *Marquette Intellect Prop Law Rev* 2007;11:379. 982

- 983 Edwards L, Harbinja E. What happens to my facebook profile  
984 when I die?": legal issues around transmission of digital  
985 assets on death. In: Maciel C, Carvalho Pereira V, editors.  
986 Digital legacy and interaction. Springer; 2013. p. 115–44.
- 987 Fernández Flores R. La ejecución de los contratos click-wrap y  
988 browse-wrap en Derecho español. *Economist&Jurist*  
989 2015;23(87):82–7.
- 990 Harbinja E. Does the EU data protection regime protect  
991 post-mortem privacy and what could be the potential  
992 alternatives. *SCRIPTed J Law Technol Soc* 2013;10(1).  
993 doi:[10.2966/scrip.100113.19](https://doi.org/10.2966/scrip.100113.19).
- 994 Harbinja E. Post-mortem privacy 2.0: theory, law and technology.  
995 *Int Rev Law Comput Technol* 2017;31(1):26–42.  
996 doi:[10.1080/13600869.2017.1275116](https://doi.org/10.1080/13600869.2017.1275116).
- 997 Hopkins JP. Afterlife in the cloud: managing a digital estate.  
998 *Hastings Sci Technol Law J* 2013;5(2):209–44.
- 999 Kutler N. Protecting your online you: a new approach to handling  
1000 your online persona after death. *Berkeley Technol Law J*  
1001 2011;26(4) [10.15779/Z38611W](https://doi.org/10.15779/Z38611W).
- 1002 Lastowka G. Virtual justice. the new laws of online worlds.  
1003 Newhaven, London: Yale University Press; 2010.
- 1004 Leaver, T. (2013). The social media contradiction: data mining and  
1005 digital death., 16(2).
- 1006 Marwick A, Ellison NB. There isn't wifi in heaven!" negotiating  
1007 visibility on facebook memorial pages. *J Broadcast Electron*  
1008 *Med* 2012;56(3):378–400. doi:[10.1080/08838151.2012.705197](https://doi.org/10.1080/08838151.2012.705197).
- 1009 Massimi, M., & Charise, A. (2009). Dying, death, and mortality:  
1010 Towards thanatosensitivity in HCI.
- 1011 Mazzone J. Facebook's Afterlife. *North Carol Law Rev* 2011;90:1643.
- 1012 McCallig D. Private but eventually public: why copyright in  
1013 unpublished works matters in the digital age. *SCRIPTed J Law*  
1014 *Technol Soc* 2013;20(1):39–56.
- 1015 McCallig D. Facebook after death: an evolving policy in a social  
1016 network. *Int J Law Inf Technol* 2014;22(2):107–40.
- 1017 McCarthy L. Digital assets and intestacy. *Boston Univ J Sci*  
1018 *Technol Law* 2015;21(2):384–412.
- McEwen RN, Scheaffer K. Virtual mourning and memory  
construction on facebook. *Bull Sci Technol Soc*  
2013;33(3–4):64–75 [10.1177/0270467613516753](https://doi.org/10.1177/0270467613516753).  
1021
- Nelson SD, Simek JW. Technology: when you die, will your digital  
assets go to hell. *Res Gestae Indiana Bar J* 2016;60.  
1022 1023
- Ray C. Til death do us part: a proposal for handling digital assets  
after death. *Real Prop Trust Estate Law J* 2012;47(3):583–615.  
1024 1025
- Ruda González A. Vida más allá de la muerte (digital). La  
protección de las voluntades digitales en la reforma del  
derecho civil catalán. Proceedings of the paper presented at  
the managing risk in the digital society. *actas del 13 °*  
congreso internacional internet, derecho y política.  
universitat oberta de catalunya, 2017.  
1026 1027 1028 1029 1030 1031
- 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).  
1032 1033 Q5
- Sofka C, Noppe Cupit I, Gilbert KR. Dying, death, and grief in an  
online universe: for counselors and educators. New York:  
Springer; 2012.  
1034 1035 1036 1037
- Subotnik EE. Copyright and the living dead?: succession law and  
the postmortem term. *Harv J Law Technol* 2015;29(1).  
1038 1039
- Sy E. The revised uniform fiduciary access to digital assets act:  
has the law caught up with technology. *Touro Law Rev*  
2016;32(3).  
1040 1041 1042
- Varnado SS. Your digital footprint left behind at death: an  
illustration of technology leaving the law behind. *Louisiana*  
*Law Rev* 2014;74(3).  
1043 1044 1045
- Walter T, Hourizi R, Moncur W, Pitsillides S. Does the internet  
change how we die and mourn? Overview and analysis.  
*Omega J Death Dying* 2012;64(4):275–302.  
1046 1047 1048
- Watkins AF. Digital properties and death: what will your heirs  
have access to after you die. *Buffalo Law Rev* 2014;62.  
1049 1050
- Wright N. Death and the internet: the implications of the digital  
afterlife. *First Monday* 2014;6(2).  
1051 1052