

# Logging off for life

Testators should plan carefully for the post-mortem management of digital assets

By BERNADETTE CAREY

Take steps now to ensure your client's online presence is managed appropriately after death.

In Australia, to date at least, there has been little, if any, recognition of the importance of estate planning for digital assets. In the absence of clear legislative guidance, solicitors should take careful, practical steps now to ensure their clients' online legacy is appropriately managed and protected after they have passed on.

## Digital assets have a multitude of forms and no expiry date

As technology continues to evolve, so too does our online presence. Profiles on Face-

book, LinkedIn and Twitter, to name just a few, now record our lives (both private and professional) as well as our thoughts, opinions and achievements in real time. While barely heard of just 10 years ago, these and other social media and online platforms are now an integral part of the lives of a significant proportion of the population.

As a result, almost all of us will have collected digital assets in some form or another. In addition to social media profiles, we have email accounts such as Yahoo! and Gmail, online storage accounts such as iCloud and DropBox,

financial accounts or payment services accessed through online banking, and photo storage accounts like Flickr. This list is far from exhaustive and will continue to expand as technological advances are made.

Unlike us mere mortals, most of our digital assets do not have an expiry date. In fact, for better or for worse, our online life can live on in perpetuity. This presents a challenge: who should have access to, manage, and deal with those digital assets once we are gone?



*Bernadette Carey is a senior associate in the Corporate and Dispute Resolution Group at Colin Biggers & Paisley.*

## Rise in litigation

The right to access digital assets of a family member after their death is becoming an increasingly hot topic internationally and there is already a growing trend of litigation involving grieving families seeking access to, for example, email accounts and Facebook profiles of a deceased relative.

The quandary over who has the right to access a deceased's digital assets has troubled courts in the US for years. As early as 2005, Yahoo! was faced with litigation after it

refused to give the family of a Marine killed in battle access to his email account to create a memorial in his honour. Yahoo! initially refused the request on the basis that their terms of service stated that the contents of a user's email account terminated upon death with no right of survivorship and no transferability.<sup>1</sup>

More recently, the trustee of an estate of a young British woman applied to a US court for orders granting access to the deceased's Facebook account. In an attempt to prove that she did not commit suicide, but rather was murdered, the trustee wished to collate evidence of her state of mind as shown through Facebook posts and messages. Facebook successfully prevented the estate from acquiring account details in reliance on local privacy legislation.<sup>2</sup>

In Australia, the courts have yet to consider issues such as these. But it is just a matter of time.

### **Who should be given post-mortem access to digital assets?**

The question of who should be given post-mortem access to digital assets is of particular importance in the context of estate planning and management. An executor of a deceased estate may have entirely legitimate reasons for seeking access to digital assets.

Some, such as online banking accounts, can hold vital information such as account and credit card details necessary for the proper administration of the estate. Many digital assets, such as Paypal and Ebay accounts, can contain funds of significant value which the executor must collect for distribution. Others, such as Kodak online photo accounts, might hold sentimental value and will be memoirs treasured by family members.

However, dealing with digital assets may not be as simple as leaving login details with a third party. This can be both

inefficient and unreliable. Sensitive information left in the wrong hands could lead to disastrous consequences – even during the testator's lifetime.

### **Online locker systems**

Recognising these difficulties, and arguably seeking to capitalise on the anxiety generally associated with death, new businesses offering

*“The testator might also consider appointing a separate ‘digital executor’ who is more comfortable with technology.”*

online and subscription-based “vaults” and “lockers” to hold passwords and other information securing digital assets have begun to spring up on the internet. Providers such as “Deathswitch”, “Legacy locker” and “iCroak” (recently rebranded as the rather more tasteful “Cirrus legacy”) trumpet slogans such as “don’t die with secrets that need to be free” and “log off in peace”.

However, as with anything online, the locker systems may themselves be the targets of online fraudsters and identity thieves and are unlikely to offer the most attractive solution.

### **Ensuring wishes for digital assets are respected**

While some formal guidance on this matter is clearly warranted, there are obvious, and complex, issues for legislators to wrestle with in the course of considering the issue of the proper management of a deceased person's digital assets. These include matters of intellectual property and privacy law, as well as debates about licensing and ownership of digital assets.

Pending the development of legislative guidance or

clear case authority, it seems the most sensible action for practitioners is also the most practical. Ensuring your client has an effective digital asset management plan might involve the testator or instructing solicitor:

- making a list of the testator's digital assets and online accounts, including every website on which the testator has an online presence;
- making a record of the user names and passwords to each account, including answers to any security questions which will allow for the password to be bypassed or changed. This information will be kept separately from the testator's will, perhaps in a safety deposit box or in a sealed envelope to be stored with you and updated from time to time;
- ensuring the testator's will contains a specific clause to allow for the testator's executors to access some or all of the testator's digital assets (as defined in the will) which refers to where the full list and password information can be found. The testator might also consider appointing a separate ‘digital executor’ who is more comfortable with technology; and
- drafting explicit instructions on how the testator wants their digital assets to be dealt with. This will involve, for example, consideration of whether the testator really wants family reading their personal emails or accessing other personal information, or whether the testator simply wants all online accounts to be deleted.

With these simple steps in place, a testator's digital identity and assets can be effectively managed after death – and they really can “log off in peace”. □

### **ENDNOTE**

1. Associated Press (2013) “Yahoo gives dead marine's family email info”, retrieved from NBC News <http://tinyurl.com/ayldv5m>.
2. Declan McCullagh (2012) “Facebook fights for deceased beauty queen's privacy”, retrieved from CNET <http://tinyurl.com/8u33bug>. □