Digital registers and estate planning

Dr Martin Gibbs**, **Dr Craig Bellamy**, **Dr Michael Arnold**, **Dr Bjorn Nansen** and **Dr Tamara Kohn
THE UNIVERSITY OF MELBOURNE

Introduction

The internet and other digital technologies are an important part of everyday life. We are, increasingly, using them to upload and download files, communicate with family and friends, store and share documents, listen to music, read books, watch videos and so forth. These files accumulate throughout life and become an important record of that life.

Digital files and assets commonly include personal emails, material on social networking sites such as Facebook, music files on services such as iTunes, images on services such as Flickr, videos on services such as YouTube, documents of many kinds on cloud storage services such as DropBox, books and newspapers on services such as Kindle, domain names and personal websites, and financial credit on services like PayPal or eBay.

An increasingly common and important question to address is: what happens to a person's digital assets and files when they die, and how can they be passed from one generation to the next?

Some of our digital files and assets may have monetary value, such as online auction, gambling and financial accounts, and some are of personal value, such as videos, documents and photos. Digital technologies are increasingly utilised in daily life and are important records of a life, especially to friends and family who wish to remember the person who has passed away. Without considering the management of these digital assets, there is danger that they may be lost, inaccessible and/or destroyed when a person dies or loses capacity.

In the same manner that estate planning is needed for the distribution of material and financial assets, it is becoming increasingly important to plan for the distribution of a person's digital material. It is important to consider who will have access to these digital files and assets and how they will be managed, passed on and/or deleted. A good way to make these preparations is through the creation of a "digital register".[1] We use the term "digital register" to refer to a private record of the account details, user names and passwords needed to access a person's digital assets and files, along with instructions on what to do with those digital materials, once the person has passed away. Usually, the digital register will be created and maintained by the person himself or herself. It should be stored safely (such in a solicitor's safe custody, safety deposit box at the bank or locked filing cabinet at home), often together with the person's will, to maintain the security and privacy of the person's digital files and assets.

In this article, we report on recommendations for creating private digital registers arising from a research project supported by the Australian Communications Consumer Action Network (ACCAN) conducted at the University of Melbourne.[2] In this project, interviews were conducted with "key informants" drawn from various professions and industry sectors that had expert knowledge of the issues surrounding the management of digital files and assets following the death of an individual. These professionals included spokespeople for various religious groups, senior executives of telecommunications companies and internet service providers, estate planning lawyers, moderators of online memorial sites and archivists. The second source of information was current research literature on death, memorialisation and digital heritage. The third source of information was the existing *Terms of Service* and policies of leading social media and telecommunication companies.

Digital files and assets

Ownership in digital environments is complex and is an important consideration in determining what can be bequeathed. Digital property may include emails, photos, blogs, websites, electronic documents and content uploaded to social media accounts.

Ownership of digital media and the conditions of posthumous access to it usually depends upon the particularities of the *Terms of Service* agreement entered into when the (now) deceased person initially signed up for that particular online service. Overarching contractual rights, intellectual property rights and various forms of copyright law further complicate the situation.

In addition, digital media may be held remotely on a server, very often in another country and in another legal jurisdiction.

While there are well-established procedures for locating, valuing and transferring ownership of physical property such as real estate, cars and books, the task of locating, accessing and distributing digital files and assets is, often, more difficult. For example, many online services (ie, Facebook, Flikr) have *Terms of Service* agreements that disallow the transferring of a person's account to another person. These companies have agreed to provide a service to a named individual and the agreement ends with that individual's death. Many years of photos, videos, text and other digital files and documents uploaded to an online service may be irretrievably lost if posthumous access to them is not arranged and local copies are unavailable.

A common-sense solution to this problem is for individuals to make a list of services (Flickr, PayPal, Facebook, Dropbox and so on), and record the relevant username and password for each service, along with instructions for friends, relatives and the executor of the will in a private digital register. Although this may be commonsense advice, it is often against the *Terms of Service* of many service providers (Gmail, Hotmail) who prohibit the transfer of username and password to a third party and forbid any person from accessing another person's account, deceased or not. These *Terms of Service* are, often, designed to protect the privacy of an individual, even in death.

Other internet service providers (particularly Australian providers such as iiNet and Telstra) allow access to user accounts and consider an individual who has been given the username and password to be an authorised agent of the owner of the account. Of course, for all practical purposes, the identification of the person using the username and password cannot be verified.

Wills and digital registers

Agencies such as the State Trustees of Victoria recommend that passwords and account locations should be recorded in a private digital register that accompanies a will. The private digital register would record the locations, usernames and passwords of online accounts, so that the digital files held in such accounts may be transferred to friends and relatives. It is also possible within a digital register to request the closure of some or all online accounts so that sensitive or irrelevant material is deleted.

Solicitors taking instructions for wills should encourage their clients to consider their digital assets. Some of the items that clients should consider when creating a private digital register are listed below.

Identify important digital files and assets

The client should be encouraged to undertake an audit of all of their digital files and assets, including the entire breadth of social networking services, cloud services, personal email accounts and blogs, photo and video storage services, online gaming accounts and all other internet services and accounts associated with an individual. These may include iTunes, Flickr, Facebook, LinkedIn, eBay, PayPal, online gaming and email accounts. Other digital assets can include domain names, blogs, websites, application software, phone apps, and data held on the cloud through services such as Amazon, Google Docs, and DropBox as well as other data storing facilities.

List locations and access methods

Clients should be encouraged to record the details needed to find digital materials and assets, as well as provide clear instructions on how to access files and groups of files, and what the client's wishes are in respect of such materials and assets on their death or incapacity. Solicitors should emphasise to their clients the importance of storing such information about locations, usernames and passwords securely, as well as ensuring that it is kept up to date. Finding and gaining access to accounts after death can be extraordinary difficult, if not impossible, without this information. Enabling a digital legacy to be disbursed or deleted, as appropriate, also reduces the possibility of identity theft and helps protect the privacy of the dead person.

As previously noted, passing on account details may be against the *Terms of Service* associated with the account. For this reason, if clients do not wish to risk breaching these *Terms of Service*, they should also be encouraged to regularly download important digital assets and files and store them in a local archive. Clients should consider whether these digital files and assets need to be stored securely and protected with encryption and password access. Valuable digital assets and files should also be backed up to prevent loss through computer failures such as a hard-disc crash. Of course, locally stored materials should be included in the client's private digital register.

It is also worth noting that in most cases music files and eBook files purchased from iTunes, Amazon, Kindle and others cannot be bequeathed. The consumer has purchased a licence to use the file while they are alive, but does not actually own it.

Nominate a digital "executor"

Clients should also be encouraged to nominate a person to manage the digital assets upon their death or incapacity. The nominated person should have the technical skills to locate and access accounts, to identify the files associated with these accounts and to carry out instructions in respect of these files. The nominated person may be the same person as the executor of the will.

Alternatively, a friend or family member may be nominated to assist in this regard. A digital register and associated instructions may be included as an appendix to a will, and like the will, it should be kept in a safe place known to the digital executor. However, for privacy and security reasons it may be desirable to ensure that the digital executor only gets assess to the digital register at the time of death and not before. Commercial service providers (for example *Security Safe* or *Legacy Locker*) offer specialist services that will store important data and passwords that allow nominated individuals to access accounts and files in the event of death or disability.

Maintenance and security of the digital register

Individual's digital profiles, the services they use and the usernames and passwords they use to access such accounts, are in constant flux. For this reason, it is important to maintain and update the information contained in a digital register regularly. It is also crucially important to ensure the security of the digital register. A digital register may contain much valuable information and unauthorised access to it can expose a person to possible breaches in privacy, theft of identity or financial assets and fraud.

Clients should be encouraged to consider the competing demands of maintaining a private digital register that can be accessed and regularly updated but which also needs to be held securely. For example, special online services are available that will store and regularly update important account details such as usernames and passwords. These services are controlled by a "master password" which can be included in a personal digital register that is stored safely in a place that is not easily accessible on a day-to-day basis such as with the client's will that is held in a solicitor's safe custody or safety deposit box at the bank. Alternatively, clients may decide to keep their private digital register locked in a filing cabinet or similar receptacle in their home, where it is secure yet easily accessible for updating.

Prepare paperwork

If accounts are to be closed upon death, most companies require a formal process in which proof of death is provided (usually a death certificate or published obituary notice) by a person authorised to act on the deceased behalf (usually the executor of the will). They may also require proof that this person is authorised to act on the deceased's behalf.

Conclusion

Given the current possibilities and limitations for bequeathing digital files and assets, the following issues should be considered when preparing instructions in a digital register:

- Decide what should happen to the content of files stored on cloud services, messages stored in email accounts, images stored in photo sharing accounts and so on. There may well be many thousands of files in these accounts, and providing individual instructions for each may be impractical. Thoughtful categorisation of files into archives is a useful thing to do for everyday purposes and will also make the job of deletion or disbursement of a digital estate much easier and more effective.
- Decide whether to create local archives (back-ups) of online personal files periodically. This is increasingly easy to do and most of the larger social media and software companies now offer download facilities that can be used for this purpose. However, once the data is downloaded and stored locally it is also important to consider its safety in terms of data security and privacy. If stored on a removable hard-disk for example, consider password protecting or encrypting the disk and keeping it in a secure place, or giving a second copy to a trusted friend or relative for safe keeping.
- Decide if an individual social media profile will be deleted or memorialised. Or, alternatively, if a memorial site should be established as a legacy. If converting or creating a memorial profile it is important to consider what content will be on display, who will be able to view it and who will be curating or moderating any posts made to the site.

The authors wish to acknowledge the support of the Australian Communications Consumers Action Network (ACCAN) grant scheme for their support of this project. For more information see: www.accan.org.au.

Dr Martin Gibbs
Senior Lecturer
The University of Melbourne
martin.gibbs@unimelb.edu.au
www.unimelb.edu.au

About the author

Dr Martin Gibbs is a Senior Lecturer in the Department of Computing and Information Systems at the University of Melbourne and a member of the university's Interaction Design Lab. He is the editor of a recent book about information technologies and civic engagement, From Social Butterfly to Engaged Citizen, published by MIT Press.

Dr Craig Bellamy
Research Fellow
The University of Melbourne
craig.bellamy@unimelb.edu.au
www.unimelb.edu.au

About the author

Dr Craig Bellamy is a Research Fellow in the Department of Computing and Information Systems at the University of Melbourne. He is founding Secretary of the Australasian Association for Digital Humanities and serves on a number of Digital Humanities program committees for major conferences and the editorial boards of key journals in the field.

Dr Michael Arnold
Senior Lecturer
The University of Melbourne
mvarnold@unimelb.edu.au
www.unimelb.edu.au

About the author

Dr Michael Arnold is a Senior Lecturer in the History and Philosophy of Science programme at the University of Melbourne. Michael is a founding committee member of the Community Informatics Research Network and a founding committee member of the Australian IEEE Society for the Social Implications of Technology.

Dr Bjorn Nansen
Research Fellow
The University of Melbourne
bjorn.nansen@unimelb.edu.au
www.unimelb.edu.au

About the author

Dr Bjorn Nansen is a Research Fellow in the Department of Computing and Information Systems at the University of Melbourne. He recently received an ARC early career researcher award to study children's domestic use of interactive media and natural interfaces.

Dr Tamara Kohn
Senior Lecturer
The University of Melbourne
tamara.kohn@unimelb.edu.au
www.unimelb.edu.au

About the author

Dr Tamara Kohn is a Senior Lecturer in Anthropology at the University of Melbourne. Her research and teaching interests include the anthropologies of the body, leisured practice and the senses; mobility and identity; personhood, memorialisation and death; and methods and ethics in ethnography.

This article was peer reviewed.

Footnotes

1. For further advice and information to assist Australian consumers in the planning, maintenance, and transfer of their digital accounts and resources see the Digital Heritage website: www.digitalheritage.net.au.
2. For the full report of this project see: C Bellamy, M Arnold, M Gibbs, B Nansen and T Kohn, "Death and the Internet: Consumer issues for planning and managing digital legacies" Australian Communications Consumer Action Network, Sydney, 2013, www.accan.org.au.