

estate planning

July 2011

studies

Estate planning for digital assets

by Gerry W. Beyer* and Kerri M. Griffin**

Only two states (Oklahoma and Idaho) have statutes that directly address digital assets in a probate context — and then only in the administration phase. Few estate planners provide digital asset planning for their clients, which may lead to significant problems as these assets are increasingly valuable and difficult to handle without proper planning. This *Study* reviews the following aspects of digital asset planning:

- Importance
- Results without planning

For hundreds of years, we have viewed property as falling into two major categories — personal property and real property. Personal property is traditionally divided further into tangible personal property, meaning items that you can see or hold, and intangible personal property, meaning items that lack physicality. Recently, a new subdivision of personal property has emerged that many label as “digital assets.” There is no real consensus about the property category in which digital assets belong. Some say that they are intellectual property; some say that they are intangible property; and others say that they can be transformed easily from one form of property to another with the click of a “print” button.¹ In actuality, some accounts that we consider “assets” are simply just licenses to use a website’s service that generally expire upon death.²

Although estate planners have perfected techniques used to transfer types of property that have been around for a long time, most estate planners have not figured out how to address the disposition of digital assets. It is important to understand digital assets and to incorporate the disposition of them into clients’ estate plans.

- Planning techniques
- Obstacles

WHAT ARE “DIGITAL ASSETS”?

Digital assets include “any online account that you own or any file that you store on your computer or that you store in the cloud.”³ Online accounts include, but are not limited to: email accounts such as Gmail, Yahoo!, and Hotmail; pictures stored online at Flickr, Picasa, Shutterfly, or Kodak EasyShare; videos or documents on YouTube, Google Docs or Scribd; websites or blogs such as TypePad,



HARRIS
PRIVATE BANK™

Michael J. Dyer
Managing Director, West Palm Beach
(561) 366-4216
michael.dyer@harrisbank.com

Harris Private Bank
777 S. Flagler Drive, Suite 140 E
West Palm Beach, FL 33401

Blogger, or WordPress; online banking, investment, and credit card accounts; PayPal; domain names from Go Daddy or Network Solutions; Web-hosting accounts; social networking accounts such as Facebook, Myspace, Twitter, and LinkedIn; online shopping accounts such as eBay or Amazon; virtual businesses; online auction houses; avatars on World of Warcraft or Second Life; professional and personal data backups; and online bill payment accounts for loans, insurance, utilities, and website hosting. Examples of the types of files many clients store on their computers include personal and business letters and other documents, photographs, videos, artwork, and music. While many of these assets do not have monetary value, many of them may have sentimental value to family members. Thus, every category of digital assets needs to be considered when drafting an estate plan.

WHY IS IT IMPORTANT TO PLAN FOR DIGITAL ASSETS?

Although most estate planners do not incorporate digital assets into their clients' estate plans, it is not because these assets are unimportant. It is because digital assets are a fairly new phenomenon, and attorneys are either unsure as to how they should be incorporated or unaware of the importance of doing so. Some of the benefits of planning for digital assets are discussed below.

To Make Things Easier on Executors and Family Members. If your clients are smart about their online lives, they have many different usernames and passwords for their accounts. This is the only way to secure identities, but this devotion to protecting sensitive personal information can wreak havoc on families upon incapacity or death.⁴ Consider A&E's *Hoarders*, a show that reveals the lives of people who cannot part with their belongings and have houses filled floor-to-ceiling with stacks of junk as a result. Although most of us find this disgusting, are we not also committing the same offense online when we create multiple email accounts, social networking accounts, websites, Twitter accounts, eBay accounts, online bill-paying arrangements, and more? Sorting through a deceased's online life for the important things can be just as daunting as cleaning out the house of a hoarder.

To make matters worse, the rights of executors,

agents, guardians, and beneficiaries with regard to digital assets are muddy. Oklahoma⁵ and Idaho⁶ recently passed laws granting personal representatives the power to deal with some of these digital assets. Although this is a step in the right direction, it is still unclear what happens if these laws conflict with service agreements.⁷ Thus, family members may have to go to court for legal authority to gain access to these accounts.⁸ Even after gaining legal authority, the company running the online account still may not acquiesce to a family member's authority without a battle.⁹

This process is complicated further if someone is incapacitated rather than deceased because that person will continue to have expenses that a deceased person would not have. Without passwords, a power of attorney alone may not be enough for the agent to pay these expenses. If no power of attorney is in place, a guardian may have to be appointed to access these accounts, and some companies will still require a specific court order on top of that before they release account information.¹⁰

To Prevent Identity Theft. In addition to needing access to online accounts for personal reasons and closing probate, family members need this information quickly so that a deceased's identity is not stolen. Until authorities update their databases regarding a new death, criminals can open credit cards, apply for jobs under a dead person's name, and get state identification cards. There are methods for protecting a deceased's identity, but they all involve having access to the deceased's online accounts.¹¹

To Prevent Content Theft. When an author publishes a piece on a blog, the author automatically obtains a copyright to that material.¹² Blog contents are protected by copyright for the life of the author, plus 70 years after the author's death.¹³ However, if family members are unaware of the blogs, or they do not have instructions or legal rights to access the blogs, these family members may be unable to protect that copyright. Other individuals may copy the deceased's work, and this content theft could go unnoticed.¹⁴

To Prevent Losses to the Estate. Some digital assets may be of value that can be lost if they go undiscovered for too long. Consider the case of Leonard Bernstein, who died in 1990, leaving the

manuscript for his memoir entitled *Blue Ink* on his computer in a password-protected file. To this day, no one has been able to break the password and access what may be a very interesting and valuable document.¹⁵

Suppose the decedent had an income-producing website or blog. The value of that site can depreciate quickly if family members are required to obtain a court order before being able to manage the site. Or suppose the decedent owned a lucrative domain name. If family members are unable to locate information regarding the domain name, they may miss the renewal deadline, losing that domain name forever.¹⁶

This concern is augmented further if the deceased or incapacitated ran a business and is the only person with access to incoming orders, the servers, customer relationship management programs, corporate bank accounts, electronic address books, and employee payroll accounts.¹⁷ Bids for items advertised on eBay may go unanswered and lost forever, and electronic bills for loans, insurance, and website hosting need to be discovered quickly and paid to prevent cancellations.¹⁸

To Avoid Losing the Deceased's Story. Most digital assets are not inherently valuable, but they are valuable to family members who extract meaning from what the deceased leaves behind. Historically, people kept special pictures, letters, and journals in shoeboxes or albums for future heirs. Today this material is stored on computers or online and is often never printed. Personal blogs and Twitter feeds have replaced physical diaries, and emails have replaced letters. Without alerting family members that these assets exist, and without telling them how to obtain access to them, the story of the life of the deceased may be lost forever. This is not only a tragedy for family members but also possibly for future historians, who are losing pieces of history in the digital abyss.¹⁹

For more active online lives, this concern also may involve preventing spam from infiltrating a loved one's website or blog site. Comments from friends and family normally are welcomed, but it is jarring to discover the comment thread gradually infiltrated with links for "cheap Ugg boots."²⁰ "It's like finding a flier for a dry cleaner stuck among flowers on a grave, except that it is much harder to remove."²¹ In the alternative, family members may

decide to delete the deceased's website against the deceased's wishes, simply because those wishes were not expressed to the family.²²

To Prevent Unwanted Secrets from Being Discovered. Sometimes people do not want their loved ones discovering private emails or messages. They may contain hurtful secrets or, maybe, just inside jokes and personal rantings. Without designating appropriate people to take care of certain accounts, the wrong person may come across this type of information.

To Prepare for an Increasingly Information-Drenched Culture. Although the principal concern today is the division of social media and email contents, the importance of planning for digital assets will increase each day. Online information will continue to spread out across a growing array of flash drives, iPhones, and iPads, and it will be more difficult to locate and accumulate. As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important. If a foundation for planning for these assets isn't set today, we may relearn the lesson that the Rosetta Stone once taught us: "There is no present tense that can long survive the fall and rise of languages and modes of recordkeeping."²³

WHAT ARE THE CURRENT DECEASED-USER POLICIES?

Many online account providers have vague policies regarding the fate of online accounts after the user's death — or no policies at all. Such policies are important because they outline steps that family members or executors must take to protect the deceased's email or social networking accounts. Some of the more popular online accounts, along with their current deceased-user policies, are described below.

Facebook: Family members either can remove the deceased's account or "memorialize" it. Memorializing means that the account continues; other Facebook members can interact with the deceased's wall; all status updates and contact information are deleted; access is restricted to confirmed friends; and future log-ins are prevented.²⁴

Hotmail: Family members either can delete the deceased's account or receive a CD-ROM of the contents of the email account after providing Hot-

mail with proper documentation.²⁵

Gmail/Google: Family members can gain access to the deceased user's account in the same manner as required by Hotmail, with the additional requirement of providing an email correspondence between the family member and the account owner.²⁶

LinkedIn: Family members can memorialize the deceased's account, meaning that profile access is restricted and messaging functionality is removed. Family members can also close the account.²⁷

Myspace: Family members can delete, remove content from, or preserve the deceased's Myspace profile after providing proof of death, the deceased's Myspace ID, and proof of relation to the deceased.²⁸

Twitter: Family members can either remove the deceased's account or receive an archive of the deceased's tweets after providing Twitter with their relationship to the deceased, the deceased's username, and a link to a public obituary.²⁹

WordPress: Family members can only obtain the deceased user's username and password when WordPress is required to release this information by law, or when WordPress "believes in good faith that disclosure is reasonably necessary to protect the property or rights of WordPress.org, third parties, or the public at large."³⁰

Yahoo! Mail: Family members cannot access the deceased's account unless a court has ordered its release. However, family members can close the account by providing Yahoo! with a copy of a death certificate.³¹

Although these deceased-user policies help to protect the deceased's accounts, they do not solve all the problems involved with handling digital assets. Because these deceased-user policies cannot ensure the proper or efficient disposition of a deceased's accounts, these accounts need to be considered when drafting an estate plan.

WHAT METHODS MAY BE USED TO PLAN FOR DIGITAL ASSETS?

There is currently no "right" answer regarding how to plan for digital assets, so attorneys should consider all the options and decide which option, or combination of options, is best for each individual client. The first step is to have clients take an inventory of all their digital assets, writing down usernames, passwords, and security questions and answers. From

there, attorneys can decide whether to utilize a will, separate document, trust, or online afterlife company.

Placing Digital Asset Information in a Will

When determining how to dispose of digital assets, one's first instinct may be to put this information in a will. However, for several reasons, a will may not be the best place for this information. Because a will becomes a matter of public record once admitted to probate, placing security codes and passwords within it could be dangerous. Further, amending a will each time that a testator changes a password would be cumbersome and expensive. And, if a client actually wishes to pass on a digital asset rather than information of how to deal with the asset, a will may not do the trick if the asset is one that will no longer exist upon death.

A will still may be useful for limited purposes with regard to transferring digital assets. Naming a digital executor in a will would be fine, as would specifying beneficiaries of specific digital assets, should your client wish to do so.³² A testator also may reference a separate document that contains detailed account information, rather than placing this information in the will itself.

Drafting a Separate Document with Digital Asset Information

Because of the privacy issues involved with placing this information in a will, drafting a separate document with all of the information may be a better idea. Have your clients make a list of all their online accounts, passwords, security questions and answers, and whether the accounts have monetary value. They can draft the document in the form of a letter to their executor or agent, listing detailed instructions for locating specific assets or information. They also need to designate which assets that they want deleted and which ones that they want passed on to family members, and whom they want to take care of such business. This document can be printed or stored on a computer, USB flash drive, or in a cloud with remote access.³³ If a client doesn't want to design his or her own loose-leaf system, the client may use an existing format such as the Beneficiary Book.³⁴

Giving a family member this information while alive and well can backfire on your clients. For

example, if a client gives his daughter his online banking information to pay his bills while he is sick, siblings may accuse her of misusing the funds.³⁵ Further, a dishonest family member would be able to steal the client's money undetected. If you decide that a separate document with digital asset information is the best route for your clients, this document should be kept in a safe place with your client's will and durable power of attorney. The document can be delivered to the client's executor upon the client's death or to an agent upon the client's incapacity.

Placing Digital Assets in a Trust

One of the most innovative solutions for dealing with digital assets is to create a revocable trust for the assets.³⁶ A trust may be a more desirable place for account information than a will because it would not become part of the public record. Further, many digital assets take the form of licenses that expire upon death.³⁷ If the trust owns the assets instead, the assets may survive the death of the grantor, enabling others to access the information.³⁸ And a trust may

be easier to amend and update than a will. When a person accumulates more digital assets, designating these assets as trust assets may be as simple as adding the word "trustee" after the owner's last name.³⁹ However, creating a revocable trust for digital assets, may be overkill for most individuals and may only be practical for those with digital assets of substantial value.

Use Online Afterlife Companies

Recently, entrepreneurs recognizing the need for digital estate planning have created companies that offer services to assist in planning for digital assets. These companies offer a variety of services to assist clients in storing information about digital assets as well as notes and emails that clients wish to send postmortem. As an estate planning attorney, you may find this additional service to be valuable and recommend one to your clients. A non-exclusive list of the different companies, the services that they offer, and the prices that they charge is set forth below in alphabetical order.

Name	Services Offered	Fee?
AssetLock (2006)	Enables users to upload documents, final letters, final wishes, instructions, important locations, and secret information to an online safe deposit box. Once the user dies and a minimum number of recipients confirm the user's death, AssetLock will release pre-designated information to the pre-designated recipients.	Yes
DataInherit (2006)	Provides users with online storage for passwords and digital documents.	No/yes
Dead Man's Switch (2008)	Enables users to write emails and designate recipients. Once user fails to respond to three emails, Dead Man's Switch releases the emails to the recipients.	No
Deathswitch (2006)	Enables users to write emails and designate recipients.	No/yes
Entrustet (2009)	Enables users to create a secure list of online accounts, designate which accounts get passed to heirs or deleted, and designate a Digital Executor.	No/yes
Estate++ (2008)	Enables users to upload important legal documents, photographs, notes, and instructions to a virtual safe deposit box.	Yes
EstateLogic (2008)	Enables users to store important documents, personal instructions, pictures, and family stories.	No/yes
GreatGoodbye (2009)	Enables users to prepare emails with attachments to be sent to recipients after death.	No/yes
If I Die	Enables users to write notes that will be sent to pre-designated recipients at death.	No
Last Post (2006)	Enables users to write emails and letters to designated recipients.	No/yes

Legacy Locker (2009)	Enables users to save all online account information in a digital safety deposit box and assign beneficiaries for each account.	No/yes
MentoMori (2010)	Enables users to store passwords, videos, and instructions and send emails to pre-designated recipients at death.	Yes
My Wonderful Life (2010)	Enables users to leave letters, instructions, information, and photographs for pre-designated recipients.	No
Parting Wishes (2000)	Enables users to draft online estate planning documents, design online memorials, create web pages about their lives, prepare final messages, document funeral wishes, and designate Keyholders to distribute this information.	Yes
SlightlyMorbid (2009)	Enables users to leave behind emails, instructions, and personal online contacts.	Yes
Vital Lock (2009)	Posthumously delivers text, videos, images, audio recordings, and links to pre-designated recipients.	No/yes

Many companies allow users to create memorial websites for loved ones. Different sites allow different content, including pictures, notes, videos, and audio recordings. Some of these companies, along with their prices, include: 1000Memories (free), BCelebrated (one month free, \$19.95 per year or \$99.95 lifetime membership), Chronicle of Life (\$10 per each 10MB), GoneTooSoon (free), Legacy.com (\$36.75 for first year and \$19 per year after), LifeNaut (free), Lifestrand (free), Memorial Gardens (free), Online Legacy/Permasite (free), RememberWell (free), SympathyTree (\$95 for first year and \$45 per year after or \$159 one-time fee), The Voice Library (\$50 for five hours of recording and listening), Virtual Eternity (free Basic Plan, \$5.95 per month Personal Plan, or \$24.95 per month Family Plan).

WHAT ARE THE OBSTACLES TO PLANNING FOR DIGITAL ASSETS?

Including digital assets in estate plans is a new phenomenon, so many of the kinks have not yet been straightened out. Some of the problem areas surrounding planning for digital assets are discussed below.

Safety Concerns. Clients may be hesitant to place all of their usernames, passwords, and other information in one place. We have all been warned never to write down our passwords. This document could fall into the hands of the wrong person, leaving your client exposed. One option to safeguard against this is to have your clients create two documents, one

with usernames and one with passwords. The documents can be stored in different locations or given to different family members. With an online afterlife management company or an online password vault, clients may worry that the security system could be breached, leaving them completely exposed.⁴⁰ The same concern is present if your client chooses to place all this information in one document.

Hassle. Another obstacle to planning for digital assets is that it is an unwanted burden. Digital asset information is changing constantly and is stored on a variety of devices (e.g., desktop computers, laptop computers, smart phones, cameras, iPads, CDs, DVDs, and flash drives). A client may open new email accounts, new social networking or gaming accounts, or change passwords routinely. Documents with this information must be revised, and accounts at online afterlife management companies must be updated frequently. For the clients who wish to keep this information in a document, tell them to update the document quarterly and save it to a USB flash drive or in the cloud, making sure that a family member knows where to locate it.⁴¹

Uncertain Reliability of Online Afterlife Management Companies. Afterlife management companies come and go. Their life is dependent upon the whims and attention spans of their creators and creditors. The lack of sustained existence of all of these companies makes it hard, if not impossible, to determine whether this market will remain viable. Clients may not want to spend money to save digital asset information when they are unsure about the reliability of the companies.⁴²

FOOTNOTES

Overstatement of Online Afterlife Management Companies' Abilities. Some of these companies purport to distribute digital assets to beneficiaries. Explain to your clients that these companies cannot do this legally and that a will is needed to transfer assets, regardless what kind. Using these companies to store information to make the probate process easier is fine, but they cannot be used to avoid probate altogether. David Shulman, an estate planner in Florida, stated that he "would relish the opportunity to represent the surviving spouse of a decedent whose eBay business was given away by Legacy Locker to an online friend in Timbuktu."⁴³

CONCLUSION

Despite the complications surrounding planning for digital assets, clients need to understand the ramifications of failing to do so. Estate planners need to understand that this is not a trivial consideration and that it is a developing area of law. Cases will arise regarding terms of service agreements, rights of beneficiaries, and the success of online afterlife management companies. States will follow the lead of Oklahoma and Idaho, enacting legislation regarding rights over digital assets of the deceased. Estate planners need to be aware of new developments. Until then, some elementary form of planning for these assets will have to do.

*GERRY W. BEYER is Governor Preston E. Smith Regents Professor of Law, Texas Tech University School of Law, Lubbock, Texas. Prof. Beyer holds a J.D. summa cum laude from Ohio State University and LL.M. and J.S.D. degrees from the University of Illinois. Previously, Prof. Beyer taught at St. Mary's University School of Law and served as a visiting professor at several other law schools, including those of Boston College, La Trobe University (Melbourne, Australia), Southern Methodist University, the University of New Mexico, and Santa Clara University. He is a frequent contributor to both scholarly and practice-oriented publications and has authored and co-authored numerous books and articles in the estate planning field. Prof. Beyer is also a regular speaker at continuing legal education programs across the nation and is a member of the American Law Institute and an Academic Fellow of the American College of Trust and Estate Counsel.

**KERRI M. GRIFFIN holds a Bachelor of Business Administration in Marketing summa cum laude, a Master of Science in Personal Financial Planning, and a J.D. summa cum laude from Texas Tech University, where she served as a Comment Editor for the *Estate Planning and Community Property Law Journal*.

- 1 Scott Zucker, *Digital Assets: Estate Planning for Online Accounts Becoming Essential (Part II)*, THE ZUCKER LAW FIRM PLLC (Dec. 16, 2010), <http://estateplanninginfoblog.com/2010/12/digital-assets-estate-planning-for-online-accounts-becoming-necessary-part-ii/>.
- 2 Steven Maimes, *Understand and Manage Digital Property*, THE TRUST ADVISOR BLOG (Nov. 20, 2009), <http://thetrustadvisor.com/tag/digital-estate-planning>.
- 3 Nathan Lustig, *Digital Estate Planning: What are Digital Assets?*, ENTRUSTET HIWI BLOG (Apr. 19, 2010), <http://blog.entrustet.com/2010/04/19/digital-estate-planning-what-are-digital-assets/>.
- 4 Andrea Coombes, *You Need an Online Estate Plan*, WALL ST. J., July 19, 2009, available at <http://online.wsj.com/article/SB124796142202862461.html>.
- 5 H.B. 2800, 111th Congress (Okla. 2010).
- 6 S.B. 1044 61st Leg. (Idaho 2011).
- 7 *New Oklahoma Law Puts Control of Deceased's Social Media Accounts in Estate Executors*, INT'L BUS. TIMES, Dec. 2, 2010, available at <http://www.ibtimes.com/articles/88106/20101202/new-oklahoma-law-puts-control-of-deceased-s-social-media-accounts-in-estate-executors.htm>.
- 8 See Jennifer Chambers, *Family Gets GI's E-Mail*, THE DETROIT NEWS, Apr. 21, 2005, available at <http://www.justinellsworth.net/email/detnewsapr.htm>.
- 9 See Coombes, *supra* note 4.
- 10 *Id.*
- 11 See Aleksandra Todorova, *Dead Ringers: Grave Robbers Turn to ID Theft*, WALL ST. J., Aug 4, 2009, available at <http://www.smartmoney.com/retirement/estate-planning/dead-ringers-grave-robbers-turning-to-identity-theft/?zone=intromessage>.
- 12 See Darren Rowse, *Copyright, Blogging and Content Theft*, PROBLOGGER, Feb. 7, 2009, available at <http://www.problogger.net/archives/2009/02/07/copyright-blogging-and-content-theft/>.
- 13 17 U.S.C. § 302(a) (2006).
- 14 John Conner, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death*, 4 EST. PLAN. & COMMUNITY PROP. L.J. (forthcoming 2011).
- 15 Helen W. Gunnarsson, *Plan for Administering Your Digital Estate*, 99 ILL. B.J. 71 (2011).
- 16 Joseph M. Mentrek, *Estate Planning in a Digital World*, 19 OHIO PROB. L.J. 195 (May/June 2009).
- 17 See Tamara Schweitzer, *Passing on Your Digital Data*, INC., Mar. 1, 2010, available at <http://www.inc.com/magazine/20100301/passing-on-your-digital-data.html>.
- 18 See Maimes, *supra* note 2.
- 19 Rob Walker, *Cyberspace When You're Dead*, N.Y. TIMES, Jan. 5, 2011, available at http://www.nytimes.com/2011/01/09/magazine/09Immortality-t.html?_r=2.
- 20 *Id.*
- 21 *Id.*
- 22 *Id.*
- 23 Ken Strutin, *What Happens to Your Digital Life When You Die?*, N.Y. L.J., Jan. 27, 2011, available at http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202479380979&What_Happens_to_Your_Digital_Life_When_You_Die.
- 24 Section 5 of Facebook's Privacy Policy, <http://www.facebook.com/policy.php> (last visited May 20, 2011).
- 25 Windows Live Solution Center, *How to Request Data from a Deceased User's Account?*, <http://windowslivehelp.com/solution.aspx?solutionid=2aa89618-2244-4187-8383->