estate planning studies®

January 2015

Estate planning for digital assets

by Gerry W. Beyer*

It is axiomatic that estate planners need to address all of a client's assets. However, many planners still overlook digital assets, 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:

- Types of digital assets
- Importance of planning
- Impediments to planning
- Planning suggestions
- Planning difficulties
- Fiduciary access to digital assets

The term "digital asset" does not have a well-established definition, for the pace of technology is faster than the law can adapt to it. Simply stated, digital assets are electronic ones and zeros; that is, information inscribed on a tangible medium or stored in an electronic or other medium and which is retrievable in perceivable form.[1] Common types of digital assets in which your client may have an interest include:

Personal. Personal digital assets include email and text messages, e-books (e.g., Kindle and Nook), word processing and pdf files, photographs, videos, music files (e.g., mp3s and iTunes), spreadsheets, PowerPoint presentations, tax records and returns, and similar materials. They may be stored on a variety of devices, such as computers, tablets, smartphones, e-readers, cameras, hard drives, memory cards, CDs and DVDs, or online in the cloud. Each of these storage techniques often requires different means of access, including user names, passwords, answers to "secret" questions, biometric data (e.g., fingerprint or retinal scan), and gestures.

Social Media. Social media assets involve interactions with other people on websites such as Facebook, MySpace, LinkedIn, and Twitter. These sites are used not only for messaging and social interaction, but they also can serve as storage for photos, videos, and other electronic files.

Financial Accounts. Many clients manage their financial affairs online, including bank and PayPal accounts, investment and brokerage accounts, bill payment (e.g., utilities, credit cards, car note payments,

mortgage payments), and income taxes. Some clients may even deal with virtual currencies such as Bitcoin.

Business Accounts. If your client is a business owner, he or she is likely to have customer databases containing names, addresses, and credit card information, along with information such as order history and pending orders. A professional such as a physician, attorney, or CPA will have client records, many of which will contain confidential information.

Other Digital Assets. Your client may own a variety of other digital assets, such as domain names, blogs, loyalty program benefits (e.g., frequent flyer miles, credit card rewards, and business discounts or vouchers), and gaming property (e.g., virtual money, avatars, or other assets earned when playing online games).

IMPORTANCE OF PLANNING FOR DIGITAL ASSETS

Assist Others Upon Death or Incapacity. When individuals are prudent about their online life, 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 and fiduciaries upon incapacity and death as their rights to access digital assets are often unclear, as discussed below. Proper planning may make this process less complicated.

Reduce 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, and get state identification cards under a dead person's name.

Prevent Financial Loss to Estate. Failure to plan for digital assets upon death and disability may cause financial loss to the estate from four perspectives. First, electronic bills for utilities, loans, insurance, and other expenses need to be discovered quickly and paid to prevent cancellations. For example, without power the furnace may not run and keep pipes in the house from freezing, or the security system may not work if the residence is burglarized. Second, the decedent may have registered one or more domain names that have commercial value. If registration of these domain names is not kept current, they easily can be lost to someone waiting to snag the name upon a lapsed registration. Third, some digital assets of value may be lost if they cannot be decrypted. 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.[2] Fourth, the client may have accumulated valuable virtual property for use in online games. For example, a planet for the Entropia Universe sold for $6 million in 2011, and a space station for the same game sold for $635,000 in 2010.[3]

Avoid Losing Personal Story. Many digital assets are not inherently valuable, but are valuable to family members who extract meaning from what the deceased leaves behind. Historically, people kept special pictures, letters, and journals in albums, scrapbooks, or shoeboxes for future generations. Today this material is stored on computers or online and often is never printed. Personal blogs and Twitter feeds have replaced physical diaries, and email messages have replaced letters. Without alerting family members that these assets exist and without telling them how to get 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.

Protect Secrets. Sometimes people do not want their loved ones discovering private emails, documents, or other electronic material. They may contain hurtful secrets, jokes and stories that are not politically correct, or personal rantings. The decedent may have a collection of adult recreational material (i.e., porn) that he or she would not want others to know had been accumulated. A professional, such as an attorney or physician, may have files containing confidential client information. Without designating appropriate people to take care of electronically stored materials, the wrong person may come across this type of information and use it in an inappropriate or embarrassing manner.

IMPEDIMENTS TO PLANNING

Terms of Service. When an individual signs up for a new online account or service, the process requires the person to agree to the provider's terms of service. Service providers typically include policies that govern what happens to the digital material on the death of an account holder, but individuals rarely read the terms of service carefully, if at all. Nonetheless, the user is at least theoretically made aware of these policies before being able to access any service. The terms of these "clickwrap" agreements are often upheld by the courts.

Ownership. A problem also may arise if the client does not actually own the digital asset but merely has a license to use that asset while alive. It is unlikely that a person can transfer to heirs or beneficiaries music, movies, and books purchased in electronic form, although the client may transfer "old school" physical records (vinyl), CDs, DVDs, books, etc., without difficulty.

Federal Law. Federal law regulates the unauthorized access to digital assets and addresses the privacy of online communication.[4] Although the statutes themselves do not directly address fiduciary access to digital assets and accounts, they create constraints for individuals attempting to plan for their digital assets and their fiduciaries.

The problem simply stated is that these acts make it criminal to access digital accounts if that access violates the user agreements. User agreements typically prohibit access by anyone other than the person who opened the account. Thus, a technical violation of the federal laws may exist when a person, even with documented permission from the account holder or state law, uses that person's user name and password to access the account.

One approach being taken by some states, which either have or are considering granting fiduciaries the ability to access accounts, is to provide by statute that provisions of user agreements that would act to restrict fiduciary access are void as against public policy. Many issues may arise, however, with these types of provisions, such as whether they improperly interfere with freedom of contract or are unconstitutional attempts to circumvent federal law.

PLANNING SUGGESTIONS

Legal uncertainty reinforces the importance of planning to increase the likelihood that an individual's wishes concerning the disposition of digital assets actually will be carried out. Furthermore, many attorneys currently do not include such planning as part of their standard set of services. They should, however, begin to do so immediately. Digital assets are valuable, both emotionally and financially, and they are pervasive.

Specify Disposition According to Provider's Instructions

Although most Internet service providers have a policy regarding what happens to the accounts of deceased users, these policies are not prominently posted, and many users may not be aware of them. In April 2013 Google took an innovative first step by creating the "Inactive Account Manager," which users may use to control what happens to emails, photos, and other documents stored on Google sites (e.g., Gmail, Google+, and YouTube). The user sets a period of time after which the user's account is deemed inactive. Once the period runs out, Google will notify the individuals whom the user specified and, if the user so indicated, share data with these users. Alternatively, the user can request that Google delete all contents of the account.

Backup to Tangible Media

The user should consider making copies of materials stored on Internet sites or "inside" devices on tangible media of some type, such as a CD, DVD, portable hard drive, or flash drive. The user can store these materials in a safe place, such as a safe deposit box, and then leave them directly to beneficiaries named in the user's will. Of course, this plan requires constant updating and may remove a level of security if the files on these media are unencrypted. However, for some files, such as many years of vacation and family photos, this technique may be effective.

Prepare Comprehensive Inventory

The client should consider creating an inventory of digital assets listing how and where they are held,

along with usernames, passwords, and answers to "secret" questions.[5] Careful storage of the inventory document is essential. Giving a family member or friend this information while alive and competent can backfire on clients. For example, if a client gives his or her daughter the online banking information to pay the client's bills when he or she is sick, siblings may accuse her of misusing the funds. Further, a dishonest family member might be able to steal the client's money undetected.

If maintaining a separate document with digital asset information is the best route for the client, this document should be kept with the client's will and durable power of attorney in a safe place. The document can be delivered to the client's executor upon the client's death or agent upon the client's incapacity. The client may consider encrypting this document and keeping the passcode in a separate location (e.g., with the client's attorney or other trusted person) as a further safeguard.

Another option is to use an online password storage service. The client then would need to pass along only one password to a personal representative or agent. This one password, however, is then extremely powerful; it unlocks the door to the client's entire digital world.

As previously discussed, remember that giving someone else the client's user name and password may be against the terms of service in the contract. Accordingly, use of the client's access information may be deemed a state or federal crime because it exceeds the access that the user agreement permits.

Provide Immediate Access to Digital Assets

A client may be willing to provide family members and friends immediate access to some digital assets while he or she is still alive. A client may store family photographs and videos on websites that permit multiple individuals to have access.

Authorize Agent to Access Digital Assets

The client may include express directions in a durable power of attorney authorizing the agent to access his or her digital accounts.[6] However, as mentioned above, it is uncertain whether the agent can use that authority in a legal manner to access the information, depending on the terms of service agreement.

Place Digital Assets in a Trust

One of the most innovative solutions for dealing with digital assets is to create a revocable trust to hold the assets.[7] A trust may be a more desirable place for account information than a will because it would not become part of the public record and is easier to amend than a will. Assuming that the asset is transferable, the owner could transfer digital property into a trust (new or existing) and provide the trustee with detailed instructions regarding management and disposition.

In addition, the client could register accounts in the name of the trust so that the successor trustee would legally (and, one hopes, seamlessly) succeed to these accounts. In addition, many digital assets take the form of licenses that expire upon death. They may survive the death of the settlor if the trust owns these accounts and assets instead. When a person accumulates more digital assets, designating these assets as trust property may be as simple as adding the word "trustee" after the owner's last name.[8]

Place 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. A will may not, however, be the best place for this information for several reasons. Because a will becomes public record once admitted to probate, placing security codes and passwords within it is dangerous. Further, amending a will each time that a testator changes a password would be cumbersome and expensive.

A will, however, is useful for limited purposes. For example, your client could specify beneficiaries of specific digital assets, especially if those assets are of significant monetary value and are transferable (that is, not merely licenses). A testator also may reference a separate document, such as the inventory discussed above, that contains detailed account information that would provide the executor with valuable information.

Because only a few states have statutes authorizing a personal representative to gain access to digital assets, it may be prudent to include a provision granting such authority in wills.[9]

Use Online Afterlife Company

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 for clients to store information about digital assets as well as notes and emails that clients wish to send postmortem. Advisors must use due diligence in investigating and selecting a digital afterlife company, as many have gone out of business or have merged with a similar firm.

PLANNING DIFFICULTIES

Safety Concerns. Clients may be hesitant to place all of their usernames, passwords, and other information in one place. We all have been warned: "Never write down your passwords." This document could fall into the hands of the wrong person, leaving the client exposed. One option to safeguard against this is to have clients create two documents, one with usernames and one with passwords. The documents can be stored in different locations or given to different individuals. With an online afterlife management company or an online password vault, clients may worry that the security system could be breached. The same concern is present if a client chooses to place all this information in one unencrypted document.

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

Uncertainties Regarding Online Afterlife Management Companies. Afterlife management companies come and go; their life is dependent on the whims and attention spans of their creators and creditors. Lack of sustained existence of all of these companies makes it hard, if not impossible, to determine whether any particular company will be in business at the time that it is needed. Clients may not want to spend money to save digital asset information when they are unsure about the reliability of the companies.

In addition, some of these companies claim that they can distribute digital assets to beneficiaries upon the client's death. Clients need to understand that these companies cannot do this legally, and that they need a will to transfer assets, no matter of what kind.

Federal Law Restrictions. At least two unresolved issues are raised by federal law. The first is whether the fiduciary is "authorized" to access the digital property pursuant to the statutes prohibiting unauthorized access to computers and computer data. A second issue is whether the fiduciary can successfully request that the provider disclose records. In this situation, the fiduciary does not go online to access the accounts but rather asks the provider for the records. Although state law may provide that the fiduciary is an authorized user and, thus, may access or request records, whether state laws may trump federal law and user agreements is an unsettled issue.

FIDUCIARY ACCESS TO DIGITAL ASSETS

State legislatures recently have started addressing the rights of executors, administrators, agents, trustees, and guardians to access digital assets. Since 2000 a few states have passed legislation relating to the power of executors and administrators to have access to and control of the decedent's digital assets. Other states are considering legislation. These statutes vary in form and substance, and their power and impact remains unclear due to the limited judicial interpretation that has occurred to date.

Existing legislation takes a variety of forms and can be divided into different "generations." Each generation is a group of statutes covering similar types of digital assets, often under an analogous access structure. The first generation, comprising California, Connecticut, and Rhode Island, covers only email accounts. Perhaps recognizing the shortcomings of such a limited definition, Indiana's

second generation statute, enacted in 2007, is more open-ended, covering records "stored electronically." The third generation statutes, enacted since 2010 in Oklahoma, Idaho, Nevada, and Louisiana, expand the definition of digital assets to include social media and micro-blogging (e.g., Twitter). States that enact the Uniform Fiduciary Access to Digital Assets Act (UFADAA) compose the fourth generation.

First Generation

The first-generation statutes, enacted as early as 2002, cover only email accounts. They do not contain provisions enabling or permitting access to any other type of digital asset.

California. The first and most primitive first generation statute was enacted by California in 2002. This statute is not specifically directed to personal representatives and simply provides: "Unless otherwise permitted by law or contract, any provider of electronic mail service shall provide each customer with notice at least 30 days before permanently terminating the customer's electronic mail address."[10] Providers are likely to provide this notice via email. Consequently, in the case of a deceased account holder, the notice will be useless unless the personal representative has rapid access to the decedent's email account and monitors it regularly.

Connecticut. Legislation enacted in 2005 requires electronic mail providers to allow executors and administrators access to or copies of the contents of the decedent's account upon showing of the death certificate and a certified copy of the certificate of appointment as executor or administrator, or by court order.[11]

Rhode Island. In 2007 Rhode Island passed the Access to Decedents' Electronic Mail Accounts Act, requiring providers to provide executors and administrators access to or copies of the contents of the electronic mail accounts of the deceased, upon showing of the death certificate and certificate of appointment as executor or administrator, or by court order.[12]

Second Generation

Indiana. In 2007 the Indiana legislature added a provision to its state code requiring custodians of records "stored electronically" regarding or for an Indiana-domiciled decedent, to release such records upon request to the decedent's personal representative.[13] The personal representative must furnish a copy of the will and death certificate, or a court order. After the custodian is notified of the decedent's death, the custodian may not dispose of or destroy the electronic records for two years. Custodians need not release records "in violation of any applicable federal law" or "to which the deceased person would not have been permitted in the ordinary course of business."

Third Generation

Oklahoma. In 2010 Oklahoma enacted legislation with a fairly broad scope, giving executors and administrators "the power . . . to take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any micro-blogging or short message service website or any e-mail service websites."[14]

Idaho. In 2012 Idaho amended its Uniform Probate Code to enable personal representatives and conservators to "[t]ake control of, conduct, continue or terminate any accounts of the decedent on any social networking website, any micro-blogging or short message service website or any e-mail service website."[15]

Nevada. In 2013 Nevada authorized a personal representative to direct the termination of email, social networking, and similar accounts. In an attempt to avoid problems with federal law, the statute provides that "[t]he act by a personal representative to direct the termination of any account or asset of a decedent . . . does not invalidate or abrogate any conditions, terms of service or contractual obligations the holder of such an account or asset has with the provider or administrator of the account, asset or Internet website."[16]

Louisiana. In 2014 Louisiana granted succession representatives the right to obtain access or possession of a decedent's digital accounts within 30 days after receipt of letters. The statute attempts to trump contrary provisions of service agreements by deeming the succession representative to be an authorized user who has the decedent's lawful consent to access and possess the accounts.[17]

Specialized State Legislation

Virginia. In 2013 Virginia granted the personal representative of a deceased minor access to the minor's digital accounts, such as those containing email, social networking information, and blogs. The personal representative assumes the deceased minor's terms of service agreement for the purposes of consenting to and obtaining the disclosure of the contents of the account.[18] This legislation is limited to minors because its chief proponent, Ricky Rash, wanted to obtain information from his son's Facebook account, which he hopes will explain why his son committed suicide.[19]

Uniform Fiduciary Access to Digital Assets Act

The National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Fiduciary Access to Digital Assets Act (UFADAA) on July 29, 2014. Below is an excerpt from the Conference's summary of UFADAA:

> UFADAA gives people the power to plan for the management and disposition of their digital assets in the same way that they can make plans for their tangible property: by providing instructions in a will, trust, or power of attorney. If a person fails to plan, the same court-appointed fiduciary that manages the person's tangible assets can manage the person's digital assets, distributing those assets to heirs or disposing of them as appropriate.
>
> Some custodians of digital assets provide an online planning option by which account holders can choose to delete or preserve their digital assets after some period of inactivity. UFADAA defers to the account holder's choice in such circumstances, but overrides any provision in a click-through terms-of-service agreement that conflicts with the account holder's express instructions.
>
> Under UFADAA, fiduciaries that manage an account holder's digital assets have the same right to access those assets as the account holder, but only for the limited purpose of carrying out their fiduciary duties. Thus, for example, an executor may access a decedent's email account in order to make an inventory of estate assets and ultimately to close the account in an orderly manner, but may not publish the decedent's confidential communications or impersonate the decedent by sending email from the account. Moreover, a fiduciary's management of digital assets may be limited by other law. For example, a fiduciary may not copy or distribute digital files in violation of copyright law, and may not access the contents of communications protected by federal privacy laws.
>
> In order to gain access to digital assets, UFADAA requires a fiduciary to send a request to the custodian, accompanied by a certified copy of the document granting fiduciary authority, such as a letter of appointment, court order, or certification of trust. Custodians of digital assets that receive an apparently valid request for access are immune from any liability for good faith compliance.
>
> UFADAA is an overlay statute designed to work in conjunction with a state's existing laws on probate, guardianship, trusts, and powers of attorney. Enacting UFADAA will simply extend a fiduciary's existing authority over a person's tangible assets to include the person's digital assets, with the same fiduciary duties to act for the benefit of the represented person or estate. It is a vital statute for the digital age and should be enacted by every state legislature as soon as possible.

As of this writing, Delaware is the only state to enact a statute "close enough" to UFADAA so that NCCUSL considers the legislation to be a UFADAA.[20] However, 28 state legislatures, bar committees, and other interested groups are studying UFADAA with an eye toward enacting it ''as is" or making changes from the subtle to the significant. It appears likely that many states will join Delaware in adopting a version of UFADAA.

CONCLUSION

Complications surround planning for digital assets, but all clients need to understand the ramifications of failing to do so. Estate planning attorneys need to comprehend fully 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 ramifications of applicable state and federal laws. Until the courts and legislatures clarify the law, estate planners

need to be especially mindful in planning for these frequently overlooked assets.

** 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 the Ohio State University and LL.M. and J.S.D. degrees from the University of Illinois. Prof. Beyer is 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.*

FOOTNOTES

1. See Uniform Fiduciary Access to Digital Assets Act § 2(9), (21). For a more expansive definition, see *Digital Assets Legislative Proposal,* Oregon State Bar (May 9, 2012).
2. See Helen W. Gunnarsson, *Plan for Administering Your Digital Estate,* 99 Ill. B.J. 71 (2011).
3. Andrea Divirgilio, *Most Expensive Virtual Real Estate Sales,* Bornrich.com (Apr. 23, 2011).
4. Stored Communications Act, 18 USC § 2701 and Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
5. Sample forms are available at http://professorbeyer.com/Digital_Assets/Digital_Estate_Information_Form_(revised_10-18-2013).pdf (prepared by Gerry W. Beyer) and http://www.digitalpassing.com/wordpress/wp-content/uploads/2012/08/DigitalAudit.pdf (prepared by James Lamm).
6. For a sample provision, see Keith P. Huffman, *Law Tips: Estate Planning for Digital Assets,* Indiana Continuing Legal Education Forum (Dec. 4, 2012), available at iclef.org/2012/12/law-tips-estate-planning-for-digital-assets/.
7. See Joseph M. Mentrek, *Estate Planning in a Digital World,* 19 Ohio Prob. L.J. 195 (May/June 2009).
8. See John Conner, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death,* 4 Est. Plan. & Comm. Prop. L.J. 301 (2011). Note that some user agreements may prohibit non-human legal entities (e.g., trusts and corporations) from purchasing licenses to digital assets.
9. For a sample provision suggested by James Lamm, see Michael Froomkin, *Estate Planning for Your Digital Afterlife,* Discourse.net (Feb. 18, 2013), available at http://www.discourse.net/2013/02/estate-planning-for-your-digital-afterlife/.
10. Cal. Bus. & Prof. Code § 17538.35.
11. Conn. Gen. Stat. § 45a-334a.
12. R.I. Gen. Laws § 33-27-3.
13. Ind. Code § 29-1-13-1.1.
14. Okla. Stat. tit. 58, § 269.
15. Idaho Code § 15-3-715(28).
16. Nev. Rev. Stat. § 143.188.
17. 24 La. Rev. Stat. § 3191.
18. Va. Code § 64.2-110.
19. See Evan Carroll, *Virginia Passes Digital Assets Law,* The Digital Beyond (Feb. 19, 2013), available at http://www.thedigitalbeyond.com/2013/02/virginia-passes-digital-assets-law/.
20. 50 Del. Code §§ 5001 through 5007.