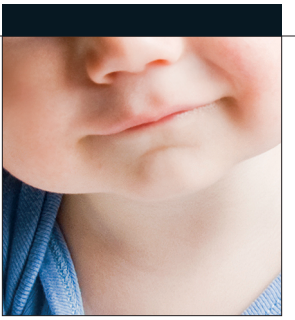

NAEPC
Journal
of Estate & Tax Planning
Click here to view the First Quarter 2015 Issue



Web Meets the Will: Estate Planning for Digital Assets

Federal and state legislation trail real-world use of digital assets, potentially increasing the difficulty of identifying and conserving these assets for heirs and beneficiaries.

GERRY W. BEYER, ATTORNEY

For hundreds of years, we have viewed personal property as falling into two major categories—tangible (i.e., items you can see or hold) and intangible (i.e., 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 many digital assets belong, as they can "switch" from one form to another such as by printing.

While 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.

Types of digital assets

The term "digital asset" does not have a well-established definition as the pace of technology is faster than the law can adapt. One of the best definitions is found in a proposed Oregon statute:

> "Digital assets" means text, images, multimedia information, or personal property stored in a digital format, whether stored on a server, computer, or other electronic device which currently exists or may exist as technology develops, and regardless of the ownership of the physical device upon which the digital asset is stored. Digital assets include, without limitation, any words, characters, codes, or contractual rights necessary to access the digital assets.[1]

Digital assets can be classified in numerous different ways, and the types of property and accounts are constantly changing. (A decade ago, who could have imagined the ubiquity of Facebook? Who can imagine what will replace it in the next few decades?) People may accumulate different categories of digital assets: personal, social media, financial, and business. An individual may also have a license or property ownership interest in the asset. Although there is some overlap, of course, clients may need to make different plans for each.

Personal. The first category includes personal assets stored on a computer or smart phone, or uploaded onto a web site such as Flickr or Shutterfly. These can include treasured photographs or videos, emails, or even playlists. Photo albums can be stored on an individual's hard drive or created through an on-line system. (They also can be created through social media, as discussed below.) People can store medical records and tax documents for themselves or fam-

GERRY W. BEYER is the Governor Preston E. Smith Regents Professor of Law at Texas Tech University School of Law in Lubbock, Texas. Portions of this article were adapted from Beyer and Cahn, "Digital Planning: The Future of Elder Law," 9 NAELA J. 135 (Spring 2013), and Beyer and Cahn, "When You Pass on, Don't Leave the Passwords Behind: Planning for Digital Assets," 26 Prob. & Prop. 40 (January/February 2012).

ily members. The list of what a client's computers can hold is, almost literally, infinite. Each of these assets requires different means of access—simply logging onto someone's computer generally requires a password, perhaps a different password for operating system access, and then each of the different files on the computer may require its own password.

Social media. Social media assets involve interactions with other people on websites—such as Facebook, MySpace, LinkedIn, and Twitter—as well as email accounts. 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. Although some bank and investment accounts have no connection to brick-and-mortar buildings, most retain some connection to a physical space. They are, however, increasingly designed to be accessed via the Internet with few paper records or monthly statements. For example, an individual can maintain an Amazon.com account, be registered with PayPal, Bitcoin, or other financial sites, have an e-Bay account, and subscribe to magazines and other media providers. Many people make extensive arrangements to pay bills online—such as income taxes, mortgages, car loans, credit cards, water, gas, telephone, cell phone, cable, and trash disposal.

Business accounts. An individual engaged in any type of commercial practice is likely to store some information on computers. Businesses collect data such as customer orders and preferences, home and shipping addresses, credit card data, bank account numbers, and even personal information such as birthdates and the names of family members and friends. Physicians store patient information. eBay sellers have an established presence and reputation. Lawyers might store client files or use a Dropbox.com-type service that allows a legal team spread across the U.S. to access litigation documents through shared folders.

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.

Domain names or blogs. A domain name or blog can be valuable, yet access and renewal may be possible only through a password or email.

Loyalty program benefits. In today's highly competitive business environment, customers have numerous options to make the most of their travel and spending habits, especially if they are loyal to particular providers. Airlines have created programs in which frequent flyers accumulate "miles" or "points" they may use towards free or discounted trips. Some credit card companies offer users an opportunity to earn "cash back" on their purchases or accumulate "points," which the cardholder may then use for discounted merchandise, travel, or services. Retail stores often allow shoppers to accumulate benefits including discounts and credit vouchers. Some members of these programs accumulate a staggering amount of points or miles and then die without having "spent" them.

The rules of the loyalty program to which the client belongs plays the key role in determining whether the accrued points may be transferred. Many customer loyalty programs do not allow transfer of accrued points upon death, but as long as the beneficiary knows the online login information of the member, it may be possible for the remaining benefits to be transferred or redeemed. However, some loyalty programs may view this redemption method as fraudulent or require that certain paperwork be filed before authorizing the redemption of remaining benefits.

Other digital assets. A client may own or control virtually endless other types of digital assets, such as "money," avatars, or virtual property in online games such as World of Warcraft or Second Life.

Importance of planning for digital assets

Planning for digital assets serves a variety of purposes.

To make things easier on executors and family members. 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 upon incapacity or death. Furthermore, 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

[1] Digital Assets Legislative Proposal, Oregon State Bar (5/9/2012).

to digital assets are unclear, as discussed below. Thus, family members may have to go to court for legal authority to gain access to these accounts. Even after gaining legal authority, the company running the online account still may not acquiesce to a family member's authority without a battle.

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.

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, and get state identification cards under a dead person's name. The methods of protecting a deceased's identity all involve having access to the deceased's online accounts.

To prevent financial losses to the estate. This reason for planning includes several areas:

- *Bill payment.* Electronic bills for utilities, loans, insurance, and other expenses need to be discovered quickly and paid to prevent cancellations. This concern is augmented further if the deceased or incapacitated ran an online business and is the only person with access to incoming orders, the servers, corporate bank accounts, and employee payroll accounts. Bids for items advertised on eBay may go unanswered and lost forever.
- *Domain names.* 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 can easily be lost to someone waiting to snag the name upon a lapsed registration.
- *Encrypted files.* 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]
- *Virtual property.* The decedent may have accumulated valuable virtual property for use in on-line games.

To avoid losing the deceased's 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 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 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.

For more active online lives, this concern may also involve preventing spam from infiltrating a loved one's website or blog site. 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.

To prevent unwanted secrets from being discovered. Sometimes people do not want their loved ones discovering private emails, documents, or other electronic material. They may contain hurtful secrets, non-politically correct jokes and stories, or personal rantings. The decedent may have a collection of adult recreational material (i.e., porn) which 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.

To prepare for an increasingly information-drenched culture. Although the principal concern today appears to be the disposition 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, smartphones, and tablets, and it will be more difficult to locate and accumulate. As

[2] See Gunnarsson, "Plan for Administering Your Digital Estate," 99 Ill. B.J. 71 (February 2011).

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 is not set today, we may re-learn the lesson 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."[3] (For 15 centuries, the meaning of the hieroglyphs on the Rosetta Stone detailing the accomplishments of Ptolemy V were lost when society neglected to safeguard the path to deciphering the writings. A Napoleonic soldier eventually discovered the triptych, enabling society to recover its writings.)

User agreements

When an individual signs up for a new online account or service, the process typically requires an agreement to the provider's terms of service. Service providers may have policies on what will happen 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. Anyone who has signed up for an online service has probably clicked on a box next to an "I agree" statement near the bottom of a web page or pop-up window signifying consent to the provider's terms of use. The terms of these "clickwrap" agreements are typically upheld by the courts.

What is in the fine print? Google's terms of service, for instance, do not include an explicit discussion of what happens when the account holder dies. In a somewhat comical provision that seems to envision Google's concern of a user coming back as a vampire or zombie, the terms provide that "upon receipt of a certificate or other legal document confirming your death, Google will close your account and you will no longer be able to retrieve content contained in that account."[4]

Google's email service, Gmail, on the other hand, does have its own policy, explained in its help section, for "Accessing a Deceased Person's Mail." Here are some of the key provisions of the policy:

> If you need access to the Gmail account content of an individual who has passed away, in rare cases we may be able to provide the contents of the Gmail account to an authorized representative of the deceased person.
>
> At Google, we're keenly aware of the trust users place in us, and we take our responsibility to protect the privacy of people who use Google services very seriously. Any decision to provide the contents of a deceased person's email will be made only after a careful review.
>
> Before you begin, please understand that Google may be unable to provide the Gmail account content, and sending a request or filing the required documentation does not guarantee that we will be able to assist you. The application to obtain email content is a lengthy process with multiple waiting periods. If you are the authorized representative of a deceased person and wish to proceed with an application to obtain the contents of a deceased person's Gmail account, please carefully review the following information regarding our two stage process.[5]

At the end of its terms of service, Yahoo! explicitly states that an account cannot be transferred: "You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted."[6]

As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important.

Facebook, the world's most popular online social network, permits someone to "Report a Deceased Person's Profile."[7] When Facebook receives proof of death through an obituary or a news article, the page can be "memorialized," so that only confirmed friends will continue to have access. Because the "wall" remains, friends can still post on the memorialized page.

Facebook "walls" are an interactive feature of a user's "profile" page which reflect the user's recent Facebook activity. Depending on user privacy settings, the wall enables a view of recent status updates, changes to the user's profile information, photos posted by or of the user, sharing links and other Internet content, and interactive comments regarding all such content between the user and his or her Facebook "friends."[8]

Ownership. A problem may also arise if the client does not actually own the digital asset but merely has

3 Strutin, "What Happens to Your Digital Life When You Die?," N.Y. L.J., 1/ 27/2011.

4 Google Terms of Service, Google Apps, #7, http://www.google.com/apps/intl/en/terms/user_terms.html (last visited 10/29/2014).

5 "Accessing a Deceased Person's Mail," Gmail Help, https://support.google.com/mail/answer/14300?hl=en (last visited 10/10//2014).

6 "Yahoo! Terms of Service," Yahoo!, #28, https://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited 10/10/2014).

7 "How do I report a deceased person or an account that needs to be memorialized?,"Facebook Help Center?, https://www.facebook.com/help/150486848354038 (last visited 10/10/2014).

8 See Miller, "Is MySpace Really My Space?: Examining the Discoverability of the Content of Social Media Accounts," 30 No. 2 Trial Advoc. Q. 28 (2011).

a license to use that asset while alive. It is unlikely 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.[9] While the statutes themselves do not directly address issues involving fiduciary's access to digital assets and accounts, they can create constraints for individuals attempting to plan for their digital assets and their fiduciaries.

Stored Communications Act. The Stored Communications Act, 18 U.S.C. section 2701(a), makes it a crime for a person to "intentionally access[] without authorization a facility through which an electronic communication service is provided." It also criminalizes the intentional exceeding of access to the facility. The Act, however, does not apply to conduct that is authorized by the user.

Section 2702 prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service, unless disclosure is made "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."

Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act, 18 U.S.C. section 1030 also prohibits unauthorized access to computers.

Interface with user agreements. Problems may arise if the terms of service prohibit a user from granting others access to the account. If a user reveals his or her user name and password and another person uses that information to access an account, it could be in violation of these acts as being without "lawful consent."

One approach being taken by some states, which either have or are considering granting personal representatives the ability to access the accounts, is to provide by statute that such access is not a breach of any terms of the user agreement. Many issues may arise, however, with this type of provision:

- Do such statutory provisions interfere with freedom of contract or already established contract rights?
- Will contrary provisions in the terms of service agreement be deemed unenforceable as against public policy?
- How will choice-of-law provisions in the user agreements, which indicate that the agreement is governed by the law of some other state or country, be handled?
- Are statutes that attempt to circumvent the federal statutes unconstitutional?

Planning suggestions

Legal uncertainty reinforces the importance of planning to increase the likelihood that an individual's wishes concerning the disposition of digital assets will be actually 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 on what happens to the accounts of deceased users, these policies are not prominently posted and many users may not be aware of them. If they are part of the standard terms of service, they may not appear on the initial screens as users quickly click through 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 such as +1s, Blogger, Contacts and Circles, Drive, Gmail, Google+ Profiles, Pages and Streams, Picasa Web Albums, Google Voice, and YouTube. The user sets a period after which the user's account is deemed inactive. Once the period runs, Google will notify the individuals 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.[10]

Back-up to tangible media. The user should consider making copies of materials stored on Internet sites or "inside" of 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

9 See Desai, "Property, Persona, and Preservation," 81 Temp. L. Rev. 67 (Spring 2008); Wilkens, "Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?," 62 Hastings L.J. 1037 (March 2011); Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 Geo. Wash. L. Rev. 1208 (2004); Hankins, "Note, Compelling Disclosure of Facebook Content Under the Stored Communications Act," 17 Suffolk J. Trial & App. Advoc. 295 (2012).

10 See "Plan your digital afterlife with inactive Account Manager," Google Data Liberation Blog, http:// dataliberation.blogspot.com/2013/04/plan-your-digital-afterlife-with.html (4/11/2013); Hill, "Will You Use Google's Death Manager to Let Loved Ones Read Your Email When You Die?," Forbes.com (4/11/2013).

safe deposit box, and then leave them directly to named beneficiaries 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 of digital estate. An initial estate planning questionnaire should include questions about the client's digital assets. While people may think of bank accounts, stock accounts, real estate, and other brick-and-mortar items as property suitable for estate planning, they may not have considered their digital assets. Accordingly, an attorney can help. In this situation, individuals need to develop an inventory of these assets, including a list of how and where they are held, along with usernames, passwords, and answers to "secret" questions. A sample form is included in Exhibit 1. Lawyers can then provide advice on what happens in the absence of planning, the default system of patchwork laws and patchy Internet service provider policies, as well as the choices for opting out of the default systems.

Careful storage of the inventory document is essential. Giving a family member or friend this information while alive and well can backfire on clients. For example, if a client gives his or her daughter the online banking information to pay the client's bills while he or she is sick, siblings may accuse her of misusing the funds. Further, a dishonest family member would 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 as a further safeguard.

Another option is to use an online password storage service such as 1Password, KeePass, or myiWallet. The client would then 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 ther client's entire digital world.

Warning. 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 to that information that is stated in the user agreement.

Provide immediate access to digital assets. A client may be willing to provide family members and friends immediate access to some digital assets while still alive. A client may store family photographs and videos on websites such as Shutterfly and DropShots, which 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. 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.

Below is suggested language:

> Digital Assets. My agent has (i) the power to access, use, and control my digital device, including, but not limited to, desktops, laptops, peripherals, storage devices, mobile telephones, smart phones, and any similar device which currently exists or exists in the future as technology develops for the purpose of accessing, modifying, deleting, controlling or transferring my digital assets, and (ii) the power to access, modify, delete, control, and transfer my digital assets, including, but not limited to, any emails, email accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, domain registrations, web hosting accounts, tax preparation service accounts, on-line stores, affiliate programs, other online programs, including frequent flyer and other bonus programs, and similar digital items which currently exist or exist in the future as technology develops.[11]

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.[12] 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. The owner could transfer digital property into a trust and provide the trustee with detailed instructions regarding management and disposition. Assuming the asset is transferable, the digital asset could be folded into an existing trust.

An individual also could set up a separate trust just to hold digital property or to hold specified digital assets. However, creating a separate revocable trust for digital assets may be overkill for many individuals and only be practical

(Text continues on page 37.)

[11] Adapted from a clause suggested by Huffman, "Law Tips: Estate Planning for Digital Assets," Indiana Continuing Legal Education Forum (12/4/2012); available at iclef.org/2012/12/law-tips-estate-planning-for-digital-assets/.

[12] See Mentrek, "Estate Planning in a Digital World," 19 Ohio Prob. L.J. 195 (May/June 2009).

EXHIBIT 1
Digital Estate Information Sample Form

I. Electronic Device Access

Device	Website	Username	PIN	Password
Computer — home				
Computer — office				
Operating system				
Voice mail — home				
Voice mail — work				
Voice mail — cell phone				
Security system				
Tablet				
e-Reader				
GPS				
Router				
DVR/TiVo				
Television				

II. E-Mail Accounts

Description	E-mail address	Username	PIN	Password	Disposition Desires
Work					
Home					
School					

III. Domain Names

Website/Domain Name	Webhost	Username	PIN	Password
Personal				
Business				

IV. On-Line Storage

Name	Website	Username	PIN	Password
Dropbox				
Google Drive				

V. Financial Software

Item	Website	Username	PIN	Password
Quicken				
TurboTax				

EXHIBIT 1, cont'd
Digital Estate Information Sample Form, cont'd

VI. Banking

Institution	Website	Username	Password	ATM PIN	Security Image
Checking					
Savings					
Paypal					

VII. Stocks, bonds, securities

Institution	Website	Username	Password	Other Information

VIII. Income Taxes

Item	Website	Username	PIN	Password
Federal income tax payment	www.eftps.com/eftps			
State income tax payment				
Prior computerized tax returns				

IX. Retirement

Institution	Website	Username	Password	Other Information

X. Insurance

Institution	Website	Username	Password	Other Information
Health				
Life				
Property				

XI. Credit Cards

Institution	Website	Username	Password	PIN
American Express				
Visa				

36

EXHIBIT 1, cont'd
Digital Estate Information Sample Form, cont'd

XII. Debts

Institution	Website	Username	Password	Other Information
Mortgage				
Cars				
Student Loan				

XIII. Utilities

Institution	Website	Username	Password	Other Information
Electric				
Gas				
Internet				
Phone (landline)				
Phone (cell)				
TV				
Trash				
Water				

XIV. Businesses

Institution	Website	Username	Password	Other Information
Amazon.com				
e-Bay.com				

XV. Social Networks

Institution	Website	Username	Password	Disposition Desires
Facebook				
LinkedIn				
Twitter				
MySpace				

EXHIBIT 1, cont'd
Digital Estate Information Sample Form, cont'd

XVI. Digital Media Accounts

Institution	Website	Username	Password	Other Information
Netflix				
iTunes				
YouTube				
Hulu				
Nook				
Kindle				

XVII. Loyalty Programs

Name	Website	Username	Password
Delta			
Southwest Airlines			
Best Buy			
Office Depot			

XVIII. Other Accounts

Name	Website	Username	Password
Skype			
LoJack			
WoW			
HalfLife			
Flickr			
Medical records			

(Continued from page 33.)

for those with digital assets of substantial value.

The client could register accounts in the name of the trust so 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 assets may be as simple as adding the word "trustee" after the owner's last name.[13]

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 a testator changes a password would be cumbersome and expensive. If a client actually wishes to pass on a digital asset rather than the information of how to deal with the asset, a will may not be the proper transfer mechanism.

A will, however, is useful for limited purposes. For example, your client could specify beneficiaries of

[13] See 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).

specific digital assets especially if those assets are of significant monetary value. A testator may also reference a separate document such as the inventory discussed above that contains detailed account information which would provide the executor with invaluable information.

If the ownership of the digital asset upon death is governed by the user agreement, the asset may actually be of the nonprobate variety. Thus, like a multiple-party bank account or life insurance policy, the digital asset may pass outside of the probate process.

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—such as the following:

> The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information. I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to the personal representative: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law. The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private.[14]

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 to assist clients in storing information about digital assets as well as notes and emails that clients wish to send post-mortem. 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.

Obstacles to planning for digital assets

Including digital assets in estate plans is a new phenomenon. Many of the kinks have not yet been straightened out. Some of the problem areas include safety issues involved with passwords, the hassle of updating this information, the uncertainty surrounding online afterlife management companies, and the fact that some online afterlife management companies overstate their abilities.

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 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, leaving them completely exposed. The same concern is present if a client chooses to place all this information in one document.

Hassle. Planning for digital assets is an unwanted burden. Digital asset information is constantly changing 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 flash drive or in the cloud, making sure that a family member,

[14] Akers, "Heckerling Musings 2013 and Other Current Developments" (February 2013), page 117; available at http://www.americanbar.org/content/dam/aba/publishing/rpte_ereport/2013/1_february/te_articles.authcheckdam.pdf.

friend, or attorney knows where to locate it.

Uncertain reliability of 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 make 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.

Overstatement of abilities of afterlife management companies. Some of these companies claim they can distribute digital assets to beneficiaries upon the client's death. Explain to clients that these companies cannot do this legally, and that they need a will to transfer assets, no matter 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.

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 request that the provider disclose records. In that situation, the fiduciary does not go online but rather asks the provider for the records. The critical question here is determining that the fiduciary becomes the subscriber for purposes of permitting access under one of the exceptions to the Stored Communications Act. While state law can clarify that the fiduciary is an authorized user, this is an issue of federal law.

Fiduciary access to digital estate

The rights of executors, administrators, agents, trustees, and guardians with regard to digital assets are muddy. Their rights in the digital world can be analogized to their rights in the brick-and-mortar world, for which there are well-established probate laws governing access, as well as established procedures designed to safeguard the power of attorney process. The practical extension of these laws to digital assets, however, is just beginning to be tested.

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 state law. Existing legislation takes a variety of forms and can be divided into different "generations." Each generation is a group of statutes covering similar (or identical) types of digital assets, often under an analogous access structure. The first generation, comprising California, Connecticut, and Rhode Island, cover 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 explicitly expand the definition of digital assets to include social media and microblogging (e.g., Twitter).

States that enact the Uniform Fiduciary Access to Digital Assets Act (UFADAA) comprise the fourth generation. At the time of this writing, Delaware is the only state that has enacted UFADAA. Note that these generations are not necessarily distinct in time, as legislation of each generational type has recently been proposed in various states.[15]

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."[16] Providers are likely to provide this notice via email. Consequently, in the case of a deceased account holder, the notice will be "wholly useless" unless the personal representative has rapid access to the decedent's email account and monitors it regularly.
- *Connecticut.* Connecticut was one of the first states to address executors' rights to digital assets. Legislation enacted in 2005 requires "electronic mail providers" to allow executors and administrators "access to or copies of the contents of the electronic mail account" of the deceased, upon showing of the death

15 See generally Mazzone, "Facebook's Afterlife," 90 N. Car. L. Rev. 1643 (2012).

16 Cal. Bus. & Prof. Code § 17538.35 (West 2010).

certificate and a certified copy of the certificate of appointment as executor or administrator, or by court order.[17]

- *Rhode Island.* In 2007, Rhode Island passed the Access to Decedents' Electronic Mail Accounts Act, requiring "electronic mail service providers" to provide executors and administrators "access to or copies of the contents of the electronic mail account" of the deceased, upon showing of the death certificate and certificate of appointment as executor or administrator, or by court order.[18]

Second generation. Perhaps in acknowledgement of changing technological times, one state has a second-generation statute which uses a broad definition of covered digital assets. While an open-ended definition may allow the law to remain relevant as new technologies are invented and new types of digital assets gain prominence, its generality may also create confusion and uncertainty as to what assets will actually be covered and how best to engage in planning for them.

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 personal decedent's personal representative.[19] 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. Third-generation legislation acknowledges the changes to the digital asset landscape, since California enacted its first generation email legislation in 2002. These third-generation laws expressly recognize new and popular digital assets—social networking and microblogging. While these laws may better serve the current population than the limited first-generation statutes, they share the same risk of becoming obsolete in only a few years.

- *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 microblogging or short message service website or any e-mail service websites."[20]
- *Idaho.* On 3/26/2012, 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 microblogging or short message service website or any e-mail service website."[21] Sponsors declared that the purpose of the bill was to "make it clear" that personal representatives and conservators can control the decedent's or protected person's "social media ... such as e-mail, blogs instant messaging, Facebook types of accounts, and so forth."[22]
- *Nevada.* Effective 10/1/2013, Nevada authorizes a personal representative to direct the termination of email, social networking, and similar accounts.[23] In an attempt to avoid problems with federal law, the statute states: "The 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."
- *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.[24]

Specialized state legislation. In 2013, Virginia enacted § 64.2-110, which grants 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.

This legislation is limited to minors because its chief proponent, Ricky Rash, wants to obtain information from his son's Facebook account, which he hopes

17 Conn. Gen. Stat. Ann. § 45a-334a (West 2012).
18 R.I. Gen. Laws § 33-27-3 (2012).
19 Ind. Code § 29-1-13-1.1 (2007).
20 Okla. Stat. tit. 58, § 269 (2012).
21 S.B. 1044, 61st Leg., Reg. Sess. (Idaho 2011).
22 Statement of Purpose, 1044–RS20153, Leg. 61, Reg. Sess. (Idaho 2011).
23 Nev. 2013 Sess. Laws ch. 325.
24 La. Rev. Stat. § 3191.

will explain why his son committed suicide.[25]

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 7/29/2014. 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 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.[26]

Future reform areas

The increasing use of digital assets heightens the need for future reform.

Providers gather user's actual preferences. Although most Internet service providers have some kind of policy on what happens to the accounts of deceased users, these policies are not prominently posted and many consumers may not be aware of them. If they are parts of the standard terms of service, they may not appear on the initial screens, as Internet users quickly click past them.

Internet service providers should follow Google's lead and develop procedures for a person to indicate what happens upon the user's death. To ensure that more people make provisions, providers should offer an easy method at the time a person signs up for a new service so the person can designate the disposition of the account upon the owner's incapacity or death.

Congress amends federal law. Ultimately, Congress will need to enact national legislation, to ensure uniformity among the states and to guarantee that Internet service providers will respect each state's forms. Such laws could use existing Internet regulation legislation as a model. Federal law could require Internet providers to respect state laws on fiduciary powers, or even to ensure that all Internet users click through an "informed consent" provision when they sign up for new services. This will at least provide default rules.

States enact UFADAA. As of the date of this writing, 28 states are studying UFADAA with an eye towards 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 success of online afterlife management companies. Until the courts and legislatures clarify the law, estate planners need to be especially mindful in planning for these frequently overlooked assets. ■

[25] See Carroll, "Virginia Passes Digital Assets Law," The Digital Beyond, 2/19/2013.

[26] 50 Del. Code §§ 5001 through 5007.