estate planning studies®

January 2018

Digital assets— A guide to planning and administration

*by Gerry W. Beyer**

Prudent estate professionals must address digital assets from two perspectives. First, they must provide for the disposition of digital assets. Second, they must provide instructions to fiduciaries regarding access to digital assets especially in light of the widespread enactment of the Revised Uniform Fiduciary Access to Digital Assets Act. This *Study* aims to provide the information you need to be well-informed about the cyberspace-estate planning interface.

■ Importance of planning ■ Planning obstacles ■ Fiduciary access ■ Planning techniques

INTRODUCTION–IMPORTANT TERMS

To have a common ground for discussing digital assets and the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), you need to be familiar with the definitions of several key terms of art.

Digital Assets

Digital assets do not refer to your client's toes and fingers. Instead, digital assets are electronic records (think binary 1's and 0's) in which a person has a right or interest. The term "digital asset" is a very broad term which encompasses all electronically-stored information, including: (a) information stored on a user's computer and other digital devices; (b) content uploaded onto Web sites; (c) rights in digital property; and (d) records that are either the catalogue or the content of an electronic communication. Examples include e-mails; text messages; photos; digital music and video; word processing documents; social media accounts (e.g., Facebook, LinkedIn, Twitter); online financial, utility, credit card, and loan accounts, and gaming avatars. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.[1]

Fiduciary

A fiduciary means a personal representative of an estate (executor or administrator), an agent under a non-medical power of attorney, a guardian of an estate, and a trustee of a trust.[2]

User

A user is a person who has an account dealing with digital assets. In our context, the user would be the decedent, principal, ward, or trustee.[3]

Custodian

The custodian is the person who carries, maintains, processes, receives, or stores a digital asset (e.g., the user's e-mail provider such as Yahoo, Google, or Suddenlink; the hosts of the user's social media accounts such as Facebook or LinkedIn; and the user's financial accounts maintained online in banks, brokerage firms, utility providers, credit card issuers, and mortgage companies).[4]

IMPORTANCE OF PLANNING

To Make Things Easier for Family Members and Fiduciaries

When individuals are prudent about their online lives, they have many different usernames and passwords for their digital assets. Each digital asset may require a different means of access—simply logging onto someone's computer or phone generally requires a password, perhaps a different password for operating system access, and then each of the different files may require its own password. Each online account is likely to have a username, password, and security questions. Some devices and apps have biometric verification, such as fingerprint scanning, iris recognition, or facial recognition.

In addition, many individuals no longer receive paper statements or bills and instead receive these materials via e-mail or by logging on to a service provider's online account. Without instructions, locating, paying/collecting, and monitoring these assets and liabilities will be a very burdensome task for the client's family members and fiduciaries.

To Prevent Identity Theft

Family members need digital asset 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.

To Prevent Financial Losses to the Estate

Bill Payment and Online Sales

Electronic bills for utilities, loans, insurance, and other expenses need to be discovered quickly and paid to prevent cancellations, foreclosures, and repossessions.

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. Estate planners should ask clients about their ownership of domain names as they may have great value. For example, Insurance.com sold for $35.6 million, Vacation-Rentals.com for $35 million, and Sex.com for $13 million.[5]

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 as far as the author can ascertain, no one has been able to break the password and access what may be a very interesting and valuable document.[6]

Virtual Property

The decedent may have accumulated valuable virtual property for use in on-line games. For example, a planet for the Entropia Universe sold for $6 million and an asteroid space resort for the same game sold for $635,000.[7] Thus, estate planners need to ask their clients a question such as, "Are you a gamer?"

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, scrapbooks, or albums for future heirs. Today, this material is stored on computers or online and often is never printed. Personal blogs and Twitter feeds have replaced physical diaries, and e-mails and texts have replaced letters. Without alerting family members that these assets exist, and without telling them how to get access to them, the life story of the deceased may be lost forever.

To Prevent Unwanted Secrets From Being Discovered

Sometimes people do not want their loved ones discovering private e-mails, documents, or other elec-

tronic 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 (porn), which he or she would not want others to know had been accumulated. A professional such as an attorney or physician is likely to 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.

OBSTACLES TO PLANNING FOR DIGITAL ASSETS

Including digital assets in estate plans is a relatively new phenomenon, and there are several obstacles that make it difficult to plan for them.

User Agreements

Terms of Service Agreements ("TOSA")

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. Anyone who has signed up for an online service probably has 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 TOSA.

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 music, movies, and books that they have purchased in electronic form, although they may transfer "old school" physical records (vinyl), CDs, DVDs, and books without difficulty.

Federal Law

There are two primary federal laws that are relevant in the discussion regarding a fiduciary's access to digital assets: (1) the Stored Communications Act ("SCA"), a federal privacy law, and (2) the Computer Fraud and Abuse Act ("CFAA"), a federal criminal law.

Stored Communications Act

The Stored Communications Act was enacted in 1986 as part of the Electronic Communications Privacy Act.[8] The SCA provides for criminal penalties to be imposed on anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[9] In addition, the SCA prohibits disclosure unless it 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."[10]

There are two significant cases worthy of mention: First, *In re Facebook, Inc*. (the *Daftary* case), decided by the Federal District Court for the Northern District of California.[11] The decedent's personal representative attempted to compel Facebook to turn over the contents of the decedent's account under the belief that the account held evidence that the decedent did not commit suicide and instead was murdered. The Court noted that under the SCA, lawful consent to disclosure may *permit* a custodian to disclose electronic communications, but it does not *require* such disclosure, and, therefore, Facebook could not be compelled to turn over the contents.

On October 16, 2017, the Supreme Judicial Court of Massachusetts became the first court to answer the question of whether a personal representative of a deceased individual may grant "lawful consent" on behalf of the deceased individual for purposes of the SCA in *Ajemian v. Yahoo!, Inc*.[12] The Court answered the question in the affirmative, firmly repudiating the position of service providers that the SCA prohibits such disclosure. However, the court's decision echoed the *Daftary* court's sentiment that even with lawful consent from a personal representative, the SCA does not require Yahoo! to disclose the decedent's e-mail account content to the personal representatives; it merely holds that the SCA *permits* the disclosure.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act also was enacted in 1986. It states that anyone who "intention-

ally accesses a computer without authorization or exceeds authorized access" has committed a crime.[13] The United States Department of Justice asserts that the CFAA allows the government to charge an individual with a crime for violating the CFAA if such individual violates the access rules of a service provider's TOSA which typically prohibit the user from granting access to others.

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." A detailed list could fall into the hands of the wrong person or an online password management company could be hacked.

Hassle

Digital asset information is changing constantly. A client may open new accounts routinely, change passwords, and purchase new devices. Accordingly, documents with this information must be revised on a regular basis.

THE REVISED FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

As of November 1, 2017, RUFADAA already has been enacted in 37 states: Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Maryland, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Wisconsin, and Wyoming. RUFADAA is pending in seven states and the District of Columbia. In addition, California enacted the decedent's estates and trusts provisions of RUFADAA.

Below is a summary of how RUFADAA operates, presented in a Question and Answer format.

Does it matter when the decedent died; the power of attorney, will, or trust executed; or guardianship opened?

No. RUFADAA applies to a fiduciary regardless of when the decedent died, the power of attorney or will executed, the guardianship commenced, or the trust created.[14]

How is priority for access to a decedent's digital assets determined?

First, priority is given to the user's instructions using the custodian's online tool; that is, the custodian's service that allows the user to provide directions for disclosure (or nondisclosure) of digital assets to a third person. Examples include Google's Inactive Account Manager and Facebook's Legacy Contact. Second priority is given to the user's instructions in the user's will, power of attorney, or trust. If the user has not provided instructions, then the service provider's terms of service agreement (the "I agree" button) will govern the rights of the decedent's personal representative. Typically, these provisions prohibit access by third parties.

Is there anything special about "access" that I need to know?

Yes! There is a major difference between two types of access. The first type is access to the contents of electronic communications, which refers to the substance or meaning of the communication, such as the subject line and text of e-mail messages. The second type of access encompasses both the catalogue of electronic communications (e.g., the name of the sender, the e-mail address of the sender, and the date and time of the message but not the subject line or the contents) and other digital assets (e.g., photos, videos, material stored on the user's computer, etc.).

I am drafting a client's will. How do I proceed with regard to digital assets?

You need to address digital assets from two perspectives. First, you need to ascertain if your client owns any digital assets that are transferable upon death. If so, you need to determine whom your client wants to receive them, just as you would any other type of property. If you do not make a specific gift of digital assets, they will pass under the residuary clause.

Second, you need to find out your client's desires regarding the executor reading the substance of e-mail messages, texts, and private social media postings. If your client wants the executor to have this access, express language granting access must be included in the will.

I am drafting a client's durable power of attorney for property. How do I proceed with regard to digital assets?

You should ask your client whether the client wants the principal to have access to the contents of electronic communications. The agent will have access to contents only if there is express language authorizing access in the power of attorney. Note that some statutory power of attorney forms provide for access unless the principal expressly removes the power. Even without contents authority, the agent may access the catalogue and non-communication digital assets.

I am applying to the court for my client to be appointed as the guardian of the estate (conservator) of a ward. How do I proceed with regard to digital assets?

Access to digital assets is not automatically granted to a guardian of the estate or conservator by virtue of the fact that the person is appointed. If there is a hearing on the matter, a court may grant a guardian complete access to the ward's digital assets. Without a hearing, a guardian may obtain access to the catalogue and digital assets other than the content of electronic communications but a court order is still required along with other specified required documentation. In addition, a guardian may also request that an account be terminated or suspended for good cause.

I am the executor of a decedent's estate. How do I get access to the contents of the decedent's electronic communications?

If a deceased user consented in the user's will, a custodian must disclose the contents of electronic communications to the personal representative if the representative provides the information required by RUFADAA, such as certified copies of the death certificate, letters testamentary, and the will containing express authorization to access contents. If the deceased user did not consent to the disclosure of contents (e.g., no express language in the will or died intestate), you will not be able to obtain access to the contents.

Before complying with the request, the custodian has the right to request additional documentation, such as: information connecting the account to the deceased user (e.g., proof that the decedent is ILoveTheLaw@yahoo.com) and a court order stating various things, including that the account actually belonged to the decedent; the disclosure of the contents would not violate the federal law; the user consented to disclosure, and disclosure is reasonably necessary for estate administration.

I am the executor of a decedent's estate. How do I get access to the catalogue of decedent's electronic communications and other digital assets?

The requirements are less stringent. Unless prohibited by the user or court order, the personal representative is granted access to the catalogue and digital assets other than the content by default upon providing the custodian with the required documentation.

Is there a practical problem for a personal representative to gain access to a decedent's digital assets?

Yes! The ability of a custodian to request a court order makes access very burdensome for personal representatives. This author has heard from representatives of Google and Facebook that they will always require a court order as they want the security of a court order before releasing any information for fear of liability for improper disclosure. Because of the likelihood that a custodian will require a court order, include the appropriate language in the earliest possible pleadings and court orders.

I am an agent for a principal. How do I get access to the contents of the principal's electronic communications?

The rules for agents are similar to those for personal representatives. Upon receiving the required documentation, a custodian must disclose the contents of electronic communications of the principal if the principal's power of attorney expressly grants the agent authority to access content.

I am an agent for a principal. How do I get access to the catalogue of the principal's electronic communications and other digital assets?

Upon receiving the required documentation, a custodian must disclose to the agent who has been granted specific authority over digital assets or general authority to act on behalf of the user the catalogue and digital assets other than content, unless otherwise ordered by the court, provided in the power of attorney, or directed by the principal.

I am a trustee. How do I obtain access to digital assets?

If the trustee is the original user, meaning that the trustee, in his or her capacity as the trustee, opened an online account or procured a digital asset, the custodian must provide the trustee with all content, catalogues, and digital assets of the trust. If the trustee is not the original user (for example, a settlor has a digital asset and then transfers it to a trust, either during life or at death), then different rules apply based on whether the trustee is requesting content or non-content material.

How long does the custodian have to comply with my disclosure request?

The custodian must comply with a request to disclose not later than 60 days after receipt of a proper request along with the required documentation.

If the user is alive, will the custodian notify the user of my request?

The custodian may, but is not required to, notify the user, e.g., the principal or ward, that a fiduciary made a disclosure request. The custodian properly may deny a disclosure request if the custodian is aware of any lawful access to the account following the receipt of the request. In other words, if the principal or ward is still using the account, the custodian may properly deny your request for access.

How does a custodian disclose the information I requested?

The custodian at its sole discretion may: grant the fiduciary full access to the user's account; limit access to the access that is sufficient for the fiduciary's performance of designated tasks; provide the fiduciary with a paper or digital copy of a digital asset; assess a reasonable administrative charge for disclosing digital assets; withhold an asset deleted by a user; and/or make the determination that a request imposes an undue burden on the custodian; and, if necessary, petition the court for an order.

What if the custodian ignores my request or refuses to disclose?

A custodian incurs no penalty for failing to disclose within 60 days of a proper request. If the custodian does not disclose, the fiduciary may apply to the court for an order directing compliance. A custodian is immune from liability for disclosing or failing to disclose if done in good faith.

Once I obtain access, what fiduciary duties do I have with regard to the information?

The legal duties imposed on the fiduciary normally also apply to digital assets, such as the duty of care, loyalty, and confidentiality.

Once I obtain proper access, am I treated as an authorized user under the law?

Yes. A fiduciary acting within the scope of the fiduciary's duties is deemed an authorized user for the purpose of applicable computer fraud and unauthorized computer access laws.

PLANNING SUGGESTIONS

Take Advantage of Online Tools

Clients should utilize the online tool option whenever it is available. Although most service providers currently do not provide an online tool option to their users, such as Google's Inactive Account Manager and Facebook's Legacy Contact. However, because so many states are enacting RUFADAA, combined with the fact that RUFADAA allows the service providers to maintain control over fiduciary access to and management of their users' accounts by creating an online tool option, we most likely will start to see more service providers creating online tools.

Backup to Tangible Media

Clients should consider making copies of materials stored on Internet sites or "inside" of devices on to tangible media of some type, such as a CD, DVD, portable hard drive, or flash drive. The client may store these materials in a safe place, such as a 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 family photos, this technique may be effective.

Prepare Comprehensive Inventory of Digital Estate

Creation

Each client should prepare a comprehensive audit of his or her digital world, including a list of how and where digital assets are held, along with usernames,

passwords, answers to "secret" questions, and what he or she would want to happen to each account in the event of disability or death. Once this inventory is created, it is just as important for clients to make sure they keep it updated when they change passwords, open new accounts, and obtain new devices. Lawyers can motivate clients to create such a digital inventory by informing them of what happens in the absence of planning, the default system of patchwork laws and patchy service provider policies, as well as the choices for opting out of the default systems.

Storage

There is a safety concern involved with this approach to planning. Careful storage of the inventory document is essential. Giving a family member or friend 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. Further, a dishonest family member would be able to steal your client's money undetected.

If you decide that a separate document with digital asset information is the best route for your client, this document could be kept with your 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. Clients can take extra steps to protect this information, such as by encrypting this document and keeping the passcode in a separate location as a further safeguard. Another option is to create two documents, one with part of the needed information, such as usernames, and one with the rest of the information, such as passwords. The documents can be stored in different locations or given to different individuals.

A newer option is to use an online password storage service such as 1Password, KeePass, or my-iWallet. Your client then would need to pass along only one password to a personal representative or agent. However, this makes this one password extremely powerful as now just one "key" unlocks the door to your client's entire digital world.

Provide Immediate Access to Digital Assets

Your client may be willing to provide family members and friends immediate access to some digital assets while still alive. Your client may store family photographs and videos on Web sites such as Flickr, GoogleDocs, DropBox, Shutterfly, and DropShot that permit multiple individuals to have access. Your client could create a family YouTube channel by using a password to protect the videos privately.

Authorize Agent to Access Digital Assets

As mentioned in the RUFADAA discussion above, the client needs to decide whether to grant the agent express authority to read the contents of e-mails, texts, and private social media postings.

Address Digital Assets in a Will

Keep in mind that a will becomes a public record once admitted to probate, so placing security codes and passwords within it is not recommended. Although a will is not an appropriate place for passwords and security codes, there are several places within a will where it might make sense to address digital assets. The discussion of RUFADAA above explains how the will needs to address both the disposition of digital assets and the access to the contents of e-mail, texts, and private social media postings.

Use Online Afterlife Company

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 e-mails that clients wish to send post-mortem. As an estate planning attorney, you may find this additional service to be valuable and recommend one to your clients. You must use due diligence in investigating and selecting a digital afterlife company. For example, in the six years that the author has been monitoring these companies, over one-third of them have gone out of business, been hacked, or merged with another similar firm.

CONCLUSION

Although complications surround planning for digital assets, all clients need to understand the ramifications of failing to do so. Estate planning professionals need to comprehend fully that this is not a trivial consideration and that it is a developing area of law. More cases will arise regarding TOSAs, rights of

beneficiaries, and the ramifications of applicable state and federal laws. The best thing clients can do at this time is to use the methods available to them to make clear their desires with regard to digital 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. Previously, Prof. Beyer served as a professor or visiting professor at Boston College, La Trobe University (Melbourne, Australia), Ohio State University, Southern Methodist University, St. Mary's University, University of New Mexico, and Santa Clara University. As a state and nationally recognized expert in estate planning and a frequent contributor to both scholarly and practice-oriented publications, Prof. Beyer was inducted into the National Association of Estate Planning Councils' Estate Planning Hall of Fame in November 2015. He is a member of the Order of the Coif, an Academic Fellow of the American College of Trust and Estate Counsel, and a member of the American Law Institute.

Portions of this *Study* are adapted from Gerry W. Beyer & Kerri G. Nipp, *Cyber Estate Planning and Administration* which is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166422. This article also contains many sample forms for digital asset planning and administration purposes.

FOOTNOTES

1. REV. UNIF. FID. ACCESS TO DIGITAL ASSETS ACT § 2(10) (2015) (hereinafter cited as "RUFADAA").
2. RUFADAA § 2(14).
3. RUFADAA § 2(26).
4. RUFADAA § 2(8).
5. *List of most expensive domain names*, Wikipedia (updated .Sept. 3, 2017).
6. *See* Helen W. Gunnarsson, Plan for Administering Your Digital Estate, 99 ILL. B.J. 71 (2011).
7. *See* Andrea Divirgilio, *Most Expensive Virtual Real Estate Sales*, Bornrich.com (Apr. 23, 2011); Oliver Chiang, *Meet The Man Who Just Made a Half Million From the Sale of Virtual Property*, Forbes.com (Nov. 13, 2010).
8. 18 USC § 2701 et seq.
9. 18 USC § 2701(a).
10. 18 USC § 2702(b)(3).
11. 923 F. Supp. 2d 1204 (N.D. Cal. 2012).
12. 478 Mass. 169 (2017).
13. 18 USC § 1030(a)(2).
14. RUFADAA § 3.