**Estate Planning and Administration in the Digital Age**

Robert R. Dunn, Esq.
Bailey Cavalieri, LLC
10 West Broad Street, Suite 2100
Columbus, Ohio 43215

## I. What are Digital Assets that a Fiduciary Needs to Administer?

### a. What is a "Digital Asset?"

The term "digital asset" refers to content stored in digital form. *See* John Romano, *A Working Definition of Digital Assets*, DIGITALBEYOND.COM (Sept. 1, 2011). Simply put, digital assets are records that are electronic. Fiduciary Access to Digital Assets Act, (National Conference of Commissioners on Uniform State Laws, Approved and Recommended July 2014). The term includes the actual content of digital records but it also encompasses catalogue information—metadata associated with that content. *Id.* For example, the content of an electronic communication would be a digital asset and so would the catalogue information associated with that communication—the identities of the people with whom the subject communicated, the time and date of communication, and the electronic address of each person involved in the communication.

### b. What is the Purpose of Obtaining Digital Assets?

In the probate context, digital assets are useful in achieving a variety of ends. First, digital assets may assist in ascertaining the intent of a testator or in preserving a will. Second, digital assets often help beneficiaries determine the value of account information. For example, electronic statements and tax forms may help beneficiaries piece together the values of various accounts and investments owned by the decedent. Third, digital assets may aid investigations into a decedent's cause of death—in both civil and criminal contexts. In one case, a California family sought access to their daughter's Facebook profile—believing that it contained information that could prove that she did not commit suicide. *In re* Request for Order Requiring Facebook, Inc. to Produce Documents and Things, No. C 12-80171 LHK (PSG) (N.D. Cal. Sept. 20, 2012) *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/5:2012mc80171/257305/22/0.pdf?s=1348220335. Finally, surviving family members often seek digital assets for purely sentimental reasons. Families may seek closure by accessing personal records, e-mails, Facebook accounts and voice messages of a deceased loved one.

### c. Examples of Digital Assets and Issues with Digital Assets in Estates

Digital assets come in many forms. It may be helpful to conceptualize digital assets in several broad categories. First, password-protected electronic communications represent one of the most prominent categories of digital assets and access to password-protected information is a primary concern of digital assets law. These communications could be valuable to executors and beneficiaries by shedding light on agreements the decedent made and exposing the intent of the parties to those agreements. Second, remote-stored information (also marketed as "the cloud") is an increasingly important category of digital assets. Many people use remote backup services to access data from

multiple devices without having to physically save and transfer the data to each device and to ensure the information on their personal or business files will not be lost if their computers are damaged or lost. Under certain circumstances, beneficiaries may find it necessary to access the cloud in order to recover the decedent's digital assets. For example, if the decedent died in a fire which also destroyed his or her computer, the surviving relatives may seek to access the decedent's remote backup account in order to recover documents, tax returns or other digitally stored assets. E-trade and other online investment and financial accounts constitute a third category of common digital assets. Some people conduct their own investments online and a sudden death or incapacity can leave a trader's investments unmonitored until a beneficiary or fiduciary can establish proper authority to take control of the accounts. Fourth, professionals are increasingly apt to conduct business enterprises entirely online. Such professions include, among others, writers, music producers, web hosts, domain name traders, bloggers and photographers. Their digitally-stored business information may be copyrighted and could be a source of revenue. Professional digital assets include products intended for the marketplace, such as completed illustrations, CAD designs, and articles. They may also include internal office documents such as company logos, presentations, and spreadsheets. Consider for example, a lawyer who drafts a will on his personal computer but forgets to move it to his office document management system. Or the solo practitioner who has his entire practice on a work computer—to which no one else has access. Access to the information and authorization for the continued operation of the online business of a decedent may create value or loss for an estate. Fifth, some digital assets are valued and sought after for purely sentimental reasons. Online photograph and video sharing accounts such as Instagram and Vine, as well as online subscriptions to genealogy trackers are good examples of digital assets that are valued for sentimental reasons. The last category consists of accounts that may retain stored value after the owner dies or becomes incompetent, including accounts for virtual currencies. These may include E-bay and Pay-pal accounts, online gaming accounts, e-book libraries and iTunes accounts. With the advent of Bitcoin, a new form of currency that is generally kept in a "digital wallet" and that often has no physical manifestation, the possibility is even greater that a decedent will leave behind a digital treasure trove.

## II. What Does a Fiduciary Need to Know about Digital Assets?

### a. How Does One Identify Digital Assets?

Absent a list provided by the decedent, a fiduciary often lacks any quick and easy methods for identifying Digital Assets. For this reason, proper planning is essential for clients who hold digital assets. Estate planners should therefore be cognizant of the possibility that a client possesses digital assets and be ready to ask the client about this. This suggestion is discussed at greater length in the section III(b).

### b. What Governs Access to Digital Assets?

#### i. Private Agreements—Terms of Service Agreements and Privacy Policies

Terms of service agreements—contracts that are non-negotiable by the user—often govern online accounts. The following are several examples of popular sites' terms of service agreements:

Gmail's user agreement states that it may grant a fiduciary access to a decedent's e-mail account, but their terms and conditions make it clear that this is at Google's discretion. Google expressly states "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." *Accessing a Deceased Person's E-mail*, GOOGLE, https://support.google.com/mail/answer/14300?hl=en (last visited Sept. 5, 2014). One of the pieces of documentation Google requires to access a decedent's Gmail account is an e-mail sent from the decedent's Gmail address to the fiduciary. *Id.*

Google does provide a service called its "Inactive Account Manager"—a system that allows users to select what will happen to their account after a period of inactivity has passed, which includes the option to authorize a third party to access the user's data. Suzanne B. Walsh, *Coming Soon to a Legislature Near You: Comprehensive State Law Governing Fiduciary Access to Digital Assets*, 8 Charleston L. Rev. 429, 439 (2014) (citing Charles Arthur, *Google Launches Tool to Help Users Plan for Digital Afterlife*, Guardian (Apr. 12, 2013, 11:47 AM), http://perma.cc/6LKK-XWTZ); About Inactive Account Manager, GOOGLE, https://support.google.com/accounts/answer/3036546?hl=en (last visited Sept. 5, 2014)

LinkedIn's user agreement provides that the user owns the content but grants to LinkedIn a license to the content and information provided. The user has a limited, revocable, nonexclusive, non-assignable license and right to access its services. The user agrees that LinkedIn may disclose information if required to do so by law or in a good faith belief that access and presentation is reasonably necessary to comply subpoena, court order, or to protect the right or property of users. LinkedIn users agree to keep their passwords secret and will not permit others to use the account. *User Agreement*, LinkedIn, https://www.linkedin.com/legal/user-agreement (Last revised Mar. 26, 2014).

Yahoo's terms of service state, "[y]ou agree that your Yahoo! Account is non-transferrable 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." *Yahoo Terms of Service*, Yahoo!, https://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (Last revised Mar. 16, 2012).

In *Ajemian v. Yahoo!, Inc.*, Yahoo! refused to accept a co-administrator's authority to access his deceased brother's Yahoo! E-mails even though the surviving brother had opened and originally shared access to the account, but had forgotten the password. 83 Mass. App. Ct. 565 (2013). The appeals court refused to enforce the provisions of the terms of service contract and remanded the case to the probate court to determine whether the e-mails were an asset of the estate and whether the Stored Communications Act (to be discussed further below) barred Yahoo! from disclosing them. *Id.* The trial court differentiated between "clickwrap" agreements, where the user must click an "agree" box, and "browsewrap" agreements, in which the terms are posted but the user need not confirm having read them. *Id.* The court ruled that, without evidence that the accountholder agreed to the terms of service, it was not enforceable against anyone, including the estate's co-administrator. *Id.*

Facebook's terms of service provide, "you will not share your password . . ., let anyone else access your account, or do anything else that might jeopardize the security of your account." *Statement of Rights and Responsibilities*, Facebook, https://www.facebook.com/legal/terms, (Last revised Nov. 15, 2013). It goes on to explain, "[i]f you violate the letter or the spirit of this statement . . . [Facebook] can stop providing all or part of Facebook to you." *Id.*

### ii. Federal Law

In addition to terms of service agreements, state and federal law also govern access to digital assets. Two federal laws directly address the issue. The Federal Computer Fraud and Abuse Act of 1984 ("CFAA") sets up criminal sanctions against those who "intentionally access a computer without authorization or exceed authorized use and thereby obtains . . . information from any protected computer." 8 U.S.C. § 1030 (2012). The term "protected computer" encompasses all computers "used in or affecting interstate or foreign commerce or communication." *Id.* at (a)(2)(C). In *United States v. Mitra*, the United States Court of Appeals for the Seventh Circuit held that any instrument used to access the internet was a "computer" under CFAA. 546 U.S. 979 (2005). Therefore, according to the Seventh Circuit, devices such as smart phones, iPads, and Kindles fall within the CFAA's definition of computer.

It is not clear how the CFAA would be applied to fiduciaries. The Department of Justice has acknowledged that the CFAA encompassed certain behavior—such as lying about one's age on an online dating site—that the DOJ considers trivial and which would not merit prosecution under the CFAA. *See Cyber Security: Protecting America's New Frontier, Hearing Before the S. Comm. On Crime, Terrorism, and Homeland Security*, 112th Cong. 7 (2011) (statement of Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice). The DOJ appears to view CFAA as a means to combat hackers, fraudsters, and those who disclose sensitive information that they are privy to as employees with access to non-public files and records. *Id.* Therefore, the DOJ may not be inclined to use the Act to prosecute unauthorized use of a decedent's computer by a surviving family member. But the conservative position would be to assume that the CFAA does impose criminal sanctions on such activity.

The Stored Communications Act ("SCA") also has implications for the handling of digital assets. The SCA prohibits electronic service providers from knowingly divulging contents of electronic communications stored by or maintained on its service. 18 U.S.C. § 2702(a). The SCA also makes it a crime for individuals, such as a fiduciary, to intentionally access electronic communications without proper authorization and imposes imprisonment and fines as penalties. *Id.* at (b)(2). Although the SCA allows disclosure with the lawful consent of the originator or an addressee or intended recipient of such communications, the language does not specifically allow for consent given by a fiduciary or assignee. *Id.* at (b)(3).

### iii. State Law

In addition to private agreements and federal law, state law also addresses digital assets. All fifty states criminalize unauthorized access to computers, systems, and networks. For example, Ohio's "Unauthorized Use of Property – Computer, Cable, or Telecommunication Property" law states,

> No person, in any manner . . . shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or

information service or other person authorized to give consent. Ohio Rev. Code § 2913.04 (2004).

Ohio currently has no state law that specifically authorizes a fiduciary to access digital assets. However, some states are starting to enact or propose legislation addressing the issue of fiduciary access to digital assets. There is much variation between the state laws regarding the scope of a fiduciary's authority. Many state laws authorize access to e-mail only. *See* Samantha D. Haworth, *Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act*, 68 U. Miami L. Rev. 535, 541-42 (2014).

## III. Planning for Digital Assets in a Technologically Changing World

### a. The Legislative Proposal: Fiduciary Access to Digital Assets Act ("FADAA"), approved and recommended July 2014

In January of 2012, the National Conference of Commissioners on Uniform State Laws authorized the drafting of a model uniform act addressing fiduciary access to digital assets. Walsh, *supra* note 4 at 440; *See also* Uniform Fiduciary Access to Digital Assets Act, (National Conference of Commissioners on Uniform State Laws, Approved and Recommended July 2014) (available at http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014jul31_UFADAA%20as%20approved%20July%202014%20for%20distribution.pdf). The stated purpose of the act is "to vest fiduciaries with the authority to access, control, or copy digital assets and accounts." UFADAA, Prefatory Note of the Drafting Committee. The UFADAA addresses four different types of fiduciaries: personal representatives of an estate, conservators for protected persons (guardians), agents acting pursuant to a power of attorney, and trustees.

Sections 1-2 of the Act provides general provisions and definitions; Sections 3-6 establish authority for personal representatives, conservators, agents, and trustees. Each fiduciary is subject to different opt-in and default rules. For example, a personal representative is presumed to have authority to access all of a decedent's digital assets unless contrary to the decedent's will or other applicable law; a conservator may access digital assets pursuant to a court order; an agent is presumed to have authority to access a principal's digital assets not subject to the protections of other applicable law, but if another law protects the assets, then the power of attorney must explicitly grant access; and a trustee may access any digital asset held by the trust unless that is contrary to the terms of the trust or other applicable law. Section 7 contains provisions relating to the rights of the fiduciary to access and exercise authority over digital assets; Section 8 addresses compliance; and Section 9 grants immunity to custodians. Sections 10-15 cover miscellaneous topics, including retroactivity, applicability, effective date and similar issues.

FADAA attempts to reconcile its provisions with other laws by defining fiduciaries as "authorized" under the SCA and the CFAA which prohibit unauthorized access to computers and computer data, as well as pursuant to any comparable state law criminalizing unauthorized access, since such statutes do not apply to authorized users. See Comment to FADAA §7. While it is unclear how FADAA and the SCA and CFAA would interact, the best solution would be if federal law were amended to provide immunity for fiduciaries who access digital assets left by decedents. Walsh, *supra* Section II.

## IV. Digital Assets and Estate Planning: Best Practices

The following suggestions are designed to assist estate planners in heading off potential complications involving digital assets. First, an estate planner should work with the client to identify digital assets—using appropriate questions in the early stages of estate planning. For example, a planner would do well to ask, "Do you blog?" "Do you own rights to digital property such as domain names?" "Do you have a personal web page linked to your persona or business?" "Do you access any accounts solely through electronic means?" "Do you use or own electronic currency such as bitcoin?" "Do you host client information on a web page?" "Do you store anything of sentimental value online or on your computer?" Second, an estate planner should encourage clients to expressly authorize a fiduciary to access and transfer digital assets in their estate planning documents—including their powers of attorney, wills, and trusts. The following language serves as an example.

1. "My Executor shall have the power to access, handle, distribute, and dispose of my digital assets."
2. "My Executor shall have the power to access, use and take control of my digital devices, including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smart phones, and any similar digital device. My Executor shall have the power to access, modify, delete, control, transfer and otherwise deal with, my digital assets, including but not limited to emails, documents, images, audio, video, software licenses, domain registrations, and similar digital files, regardless of the ownership of the physical device upon which the digital asset is stored. My Executor shall have the power to access, modify, delete, control, transfer and otherwise deal with, my digital accounts, including but not limited to e-mail accounts, social network accounts, social media accounts, file sharing accounts, financial management accounts, domain registration accounts, domain name service accounts, web hosting accounts, tax preparation service accounts, online stores, affiliate programs, and other online accounts."
3. "The Trustee shall have the power to access, handle, distribute, and dispose of digital assets that comprise a portion of the trust estate."
4. "The Trustee shall have the power to access, use and take control of digital devices that comprise a portion of the trust estate, including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smart phones, and any similar digital device. The Trustee shall have the power to access, modify, delete, control, transfer and otherwise deal with, digital assets that comprise a portion of the trust estate, including but not limited to emails, documents, images, audio, video, software licenses, domain registrations, and similar digital files, regardless of the ownership of the physical device upon which the digital asset is stored. The Trustee shall have the power to access, modify, delete, control, transfer and otherwise deal with, any digital accounts that comprise a portion of the trust estate, including but is not limited to e-mail accounts, social network accounts, social media accounts, file sharing accounts, financial management accounts, domain registration accounts, domain name service accounts, web hosting accounts, tax preparation service accounts, online stores, affiliate programs, and other online accounts."
5. "My Agent can continue, transfer, terminate, and otherwise have full access and control over all my digital assets. My Agent shall have authority to obtain access to all digital accounts and to obtain all passwords and access codes. Digital assets include, but are not limited to, all social networking (such as Facebook and LinkedIn) and email accounts, as well as online bank, stock and financial accounts, Web sites, blogs, and any other information that exists in digital media

such as address books and client lists." Susan Porter, *Digital Estates: Handling Digital Assets in the Real World*, 4 PRAC. LAW. 35, 53-54 (2013).

Practitioners should encourage clients to make a digital asset inventory. This should include the web address or physical location of any digital asset, usernames and passwords to access the information. Consider keeping a flash drive with the digital inventory. Encourage clients to review their e-mail subscriptions to know their options for including and authorizing other users. If a client amasses significant value in digital assets, conduct a "valuation" as part of the estate planning strategy. The valuation should be repeated regularly, as with any other asset. Consider software such as SecureSafe and PasswordBox, which stores and organizes multiple passwords. And, for clients who operate businesses electronically, encourage them to make business plans and resolutions that specifically address the authority of the members of the company to access the digital assets (as part of the dissolution/succession plan). Consider complexities with use restrictions. Must the digital asset be terminated on the owner's death? Can a decedent create a future interest in a digital asset? When the asset is a domain name or a bitcoin wallet, can the decedent allow a beneficiary a "life estate" with ownership retained in trust? Finally, make sure certifications of trust include digital asset authorizations for purposes of presentation to a digital asset account custodian.

As society confronts rapid changes in technology, attorneys practicing in the personal planning area will need to stay abreast of these changes and adapt their practices to conform to the realities of these sweeping changes and their impact on planning and decedents' estates. While somewhat daunting, it is no doubt an exciting time to be a practitioner in this area.