*Thought Leadership*

# Digital Assets in Estate Administration: Concerns and Considerations for Fiduciaries

*Lauren G. Barron, Esq., and Samantha L. Heaton, Esq.*

*Estate fiduciaries increasingly encounter "digital assets" in estate administrations. Digital assets are electronically stored information, which may have sentimental value (such as photo files), monetary value (such as a blog that generates advertising revenue), or both. For estates with digital assets, fiduciaries should properly value such assets and report the values to the Service and in the probate filings. But the unique characteristics of digital assets—including that many are subject to the terms and conditions of terms of service agreements—create challenges in accounting for this new category of assets. Fiduciaries are also subject to potential liability for attempting to gain access to a decedent's digital accounts and property. The federal anti-hacking laws contained in the Computer Fraud and Abuse Act (as well as individual state's anti-hacking laws) and the federal privacy protection laws contained in the Stored Communications Act create obstacles for fiduciary access. For example, fiduciary use of a decedent's password to access an e-mail account may expose the fiduciary to both civil and criminal liability. Despite these challenges, certain steps taken during a person's life can ease the transfer of digital assets at death.*

## Introduction

As we become more connected over electronic media, our estate assets are changing in ways that reflect our electronically managed and transacted lives.

Digital assets are increasingly commonplace in estates, and estate fiduciaries are now faced with valuation and access questions for a new category of assets that exhibit characteristics not traditionally encountered.

The following discussion addresses what digital assets are, how to approach the valuation of these assets, how to gain access to these assets, why fiduciaries should exercise caution before obtaining access, and the preventative measures that may be implemented during the taxpayer's life in order to ensure the smooth administration of such assets at the time of death.

## Defining "Digital"

Digital assets consist of information that is electronically stored or accessed on a computing device. The information may be stored on hardware (such as your home computer or a flash drive) or in online user accounts for services such as social networking and media sites, blogs, cloud storage, and banking services. In the online context, a digital asset may include an entire website or web service, as well as the content stored there. Website domain names are also digital assets.

Defining digital assets is like trying to draw a circle around ants on the sidewalk—the boundaries are constantly changing. The Uniform Law Commission drafting committee for the Uniform Fiduciary Access to Digital Access Act (UFADAA) (to Minnesotans like us, the "uff-da" . . . but we digress) has taken a broad

approach by defining "digital asset" simply to mean: "an electronic record."[1]

The definition is qualified to the extent that "[t]he term does not include an underlying asset or liability unless the asset or liability is itself an electronic record."[2]

## Digital Assets, Tangible Value

Digital assets matter in the estate planning context because many of these assets have value. Such value may be monetary, sentimental, or both. Evidencing monetary value, a global survey sponsored by the computer security firm McAfee asked respondents to assign value to their electronically stored files, which included personal memories (such as photographs), personal records, career information, hobbies and projects, personal communications (such as e-mail), and entertainment files (such as music and movies).

The McAfee survey found that average North American respondents perceived the total value of their digital assets to be $54,722. European respondents averaged a perceived total value of $28,461, Australian respondents averaged a perceived total value of $20,948, and Japanese respondents averaged a perceived total value of $23,938.[3]

The people with valuable digital assets are not just the owners of major websites—they may be your clients who blog on the weekends or your neighbors who sell their homemade goods online; they may be you. PayPal and Amazon users, for example, may have outstanding balances and credits on those websites at any time.

In an anecdote from personal experience, a teacher who left her profession to raise her children has replaced her income with the advertising revenue generated from her blog about raising children at home.

For the virtual "gamers" out there, currencies such as BitCoin and real estate in virtual worlds such as Second Life are trading for real-world value. OKCoin, the largest Bitcoin exchange, transacted close to 1.6 million Bitcoins in May 2014, equivalent in value to approximately $1.0 billion USD.[4]

## Gift and Estate Tax Valuation

Digital assets introduce a new category of asset reporting for fiduciaries charged with administration of an estate. Digital property with financial value should be included on estate tax returns and fiduciary inventories or accountings. Such assets are valued like all others, under Section 2031(a) and Treasury Regulation 20.2031-1(b), based on fair market value as would be determined in an arm's-length transaction between a willing buyer and seller.

For digital assets that generate income, cash flows from advertisements or royalties may be used to determine value. Certain discounts for the loss of a key person (for example, a decedent who maintained a blog) or for lack of marketability may apply, as well. If the asset can be sold, an auction-based sale may yield a higher transaction price than a fixed-price sale. Certain hardware can be appraised.[5]

Qualified valuation experts should be retained to confirm value, as would be the case with any other asset that has negotiable market value. While certain web-based appraisal services are growing, these services are unlikely to use a proper valuation technique for tax purposes. Instead, it is best to retain an expert with experience in valuation for tax purposes and discuss the particularities of a specific digital asset with him or her.[6]

Fiduciaries should also be aware that the Service is using access to online data to investigate taxpayers' real estate holdings, transactions and business activities. Any digital footprint left by a decedent may surface in an audit communication from the Service.

## Digital Keys to Estate Administration—Where to Look for Them

In an estate administration, access to digital assets is likely necessary to account for all of the estate assets. Watching a decedent's mail box (the kind where paper is deposited) will no longer uncover most accounts, investments, or liabilities. Instead, an estate executor now monitors the mail by opening the decedent's laptop and viewing the decedent's "favorites" or "bookmarks" in an online browser to find existing accounts. Financial software for budgeting and taxes, whether on a local drive or online, may also reveal assets to report on an estate tax return.

## Access to the Assets

But even if the executor can determine what digital assets a decedent possessed at the time of death and where they are located, the executor may not be able to access the asset. Several obstacles outlined below chart a difficult course for executors in this situation.

## Passwords and Encryption

The first hurdle to accessing digital information may be as simple as knowing the password to open it. These ubiquitous, nonsensical little words and phrases often prevent users themselves from accessing their own information (who hasn't clicked on the "forgot my password" link?), and may be the end of the road for some fiduciaries.

Without a password, internet service providers are unlikely to grant access to online accounts, even to an attorney-in-fact appointed under a valid power of attorney or to a personal representative of an estate. Some providers, however, may provide the contents of an account if asked, although they are not required by law to do so.

The only way to insure against this obstacle is for the decedent to have planned ahead for the transfer of his or her digital assets—a topic addressed at the end of this discussion.

But even when a password is known, an executor—or anyone else for that matter—should think carefully before using it. The criminal and civil liabilities that could arise may be as severe as they are unanticipated.

## Fiduciaries May Violate Anti-Hacking Laws When They Use a Decedent's Login Credentials

Anti-hacking laws are designed to prevent unauthorized access of accounts. In the estate administration arena, anti-hacking laws present a strong barrier to fiduciary access of digital assets. This is because they arguably prohibit fiduciary access to such accounts, even when the fiduciary possesses the requisite login information.

The federal Computer Fraud and Abuse Act (CFAA) criminalizes anyone who "exceeds authorized access" in order to access digital accounts.[7] In addition to the flagrant examples of computer hacking, unauthorized access may also encompass violation of a website's access rules as described in the terms of service. For example, Facebook's terms of service agreement prohibits the use of another user's login credentials, even with permission from such user.[8]

Thus, when a fiduciary logs into to an account using a decedent's login credentials, such access may violate the terms of service and thereby also violate the CFAA.

Many find the idea that logging into a spouse's account could be a felony disturbing. In testimony before Congress, Richard Downing, the Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, stated, "Let me be very clear that DOJ is in no way interested in bringing cases against people who lie about their age on a dating site or anything of the sort."[9]

However, he also indicated that the CFAA does permit such prosecutions and argued that Congress should not impair the flexibility of the Department of Justice to address computer crimes "based on unsubstantiated fears that the Department will expend its limited resources on trivial cases such as prosecuting people who lie about their age on an Internet dating site."[10]

Leaving the matter to prosecutorial discretion may not provide much comfort to fiduciaries who wish to avoid even the whiff of wrongdoing, as well as potential liability. In particular, some may doubt the wisdom of trusting prosecutorial discretion based on the recent prosecution of Aaron Swartz, the co-founder of Reddit, who tragically committed suicide in the wake of his prosecution for CFAA violations. The aggressive prosecution was largely interpreted as partially based on a terms of service violation.[11]

In the past year, the Department of Justice has softened its stance and indicated a willingness to work with Congress to limit the ability to prosecute minor CFAA violations.[12]

Regardless of the current Justice Department interpretation of the CFAA, some courts have given a narrow reading to the statute.[13] In *U.S. v. Nosal*, the 9th Circuit considered a challenge to an employee's unauthorized *use* of information that the employee was authorized to access. The court held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions," and is therefore limited to *access* restrictions.[14]

Although *Nosal* involved the misuse of computer data to which an employee already had authorized access, the case indicated the court's general unwillingness to read the CFAA expansively.

## Privacy Laws Limit Fiduciaries' Ability to Compel Disclosure of Account Contents

The second statutory obstacle to fiduciary access of digital assets is the many internet privacy protection laws, both at the state and federal level. The federal Stored Communications Act (SCA) was enacted as part of the Electronic Communication Privacy Act of 1986, and is better known for its wiretapping provisions.[15]

The SCA prohibits internet service providers from disclosing account contents to private persons. General account information is subject to fewer disclosure limitations. For example, information about the type of e-mail account the decedent had receives fewer protections than the actual content of the e-mails. Furthermore, the SCA privacy protections only cover communications in accounts that are restricted in some fashion. Thus, information that is already public may be freely disclosed by service providers.

A few narrow exceptions permit a service provider to disclose account contents. The most significant exception is the lawful consent exception, which permits service providers voluntarily to disclose account contents when the sender or recipient consents to such disclosure.[16]

Lawful consent becomes a thorny issue in the context of estate administration. Although personal representatives are generally viewed as having the authority to access a decedent's accounts, this authority is based on state law. To the extent that federal law, such as the SCA conflicts with state law, federal law will of course prevail. As it stands, the boundaries of "lawful consent" under the SCA have not been fleshed out. Therefore, it is currently unclear whether personal representatives and other fiduciaries have the requisite lawful consent of the account holder to disclose the account contents.

Regardless of the eventual interpretation of lawful consent, such consent only permits disclosure by service providers; it can never compel disclosure. This issue was litigated in *In re Facebook, Inc.*, in which a decedent's family sought to compel Facebook's release of certain account contents.[17]

The court held that the SCA allowed only voluntary disclosure and that a service provider could not be required to disclose account contents. The court declined to rule on whether the personal representative possessed lawful consent on jurisdictional grounds, though the court noted that Facebook could conclude on its own that the personal representative had the lawful consent of the decedent. This would permit Facebook to voluntarily disclose the account contents, if it so wished. Facebook declined to do so, however.

## New State and Uniform Laws Attempt to Clarify Fiduciaries' Authority to Access Digital Assets

A handful of states have attempted to address these concerns by statutorily granting fiduciaries some degree of access to digital assets, though these laws are not addressed in this article. The Uniform Law Commission has also taken up the challenge.

The Uniform Law Commission approved the UFADAA at its annual meeting this July. The UFADAA, if adopted by a state, would clarify that fiduciaries have the authority effectively to step into the decedent's shoes so as to access digital assets and accounts. The UFADAA also attempts to overcome the obstacles of anti-hacking and data privacy laws.[18]

Under the UFADAA, a fiduciary is an "authorized user" as the term is used in applicable computer fraud and unauthorized access laws, including the CFAA. If effective, this provision would allow fiduciaries to use login credentials as an authorized user. Additionally, the UFADAA voids any limitations put on a fiduciary's access to digital assets by a terms of service agreement.

The UFADAA further provides that a fiduciary's accessing of digital assets of an account holder does not violate a terms of service agreement. These provisions reshape the effect that terms of service agreements may have under the CFAA. These provisions eliminate the potential that, by violating a terms of service agreement, a fiduciary may also violate the CFAA.

However, these UFADAA provisions will be effective only to the extent that courts interpret the CFAA in the same vein and do not find that state laws are ineffective in reshaping the contours of the CFAA.[19]

Furthermore, the effectiveness of the UFADAA relies heavily on California, where many internet companies are based, adopting the UFADAA. The UFADAA tries to soften the importance of California's adoption of the act by including a provision that makes some choice-of-law provisions in terms of service agreements unenforceable. Again, the effectiveness of this provision will be left to the courts.[20]

The UFADAA also provides that fiduciaries have the lawful consent of the account holder for the service provider to disclose the contents of an electronic communication to the fiduciary. Whereas the "authorized user" provision addresses the concerns the CFAA raises, this lawful consent provision speaks to the obstacles presented by the SCA.

The fiduciary possession of lawful consent would allow the service provider to disclose information without violating the SCA. This is because the lawful consent exception would apply. Of course, even with lawful consent so clarified, the fiduciary cannot compel a disclosure by the service provider.[21]

## Planning Ahead

Although the legal landscape continues to present challenges for access to digital information after a person dies, much difficulty can be avoided by steps taken during life. Counsel may find it useful to walk clients through a scenario of the disposition of the client's digital assets upon death.

Some mindfulness regarding what assets exist, who has access to them, and what should be preserved upon death is the first step toward creating a transfer plan. More specifically, clients may consider the following when planning ahead.

### 1. Create an Inventory

Once digital assets are identified, it is advisable to create an inventory of where they are located (web addresses, etc.) and how to access them (passwords, security question answers, etc.). This inventory will of course contain highly sensitive information.

A best practice for storing the list is to create the list electronically, either in a local software program such as Excel or in one of the website services that have emerged for this purpose. That electronic list should be encrypted with a password that is written down (on a piece of paper!) and shared with a trusted friend or fiduciary.

If your client opts to create an inventory using a website service, several issues to consider are as follows:

1. Is the list stored locally or in the cloud?
2. Is there an opportunity to designate a person to receive the inventory upon death or incapacity?
3. Will the list automatically update as I change my passwords?

At least one company, PasswordBox (formerly Legacy Locker), offers an online system for storing passwords and designating a beneficiary for each account.[22] Users should beware that such beneficiary designations may be ineffective due to a terms of service agreement governing a particular digital asset or may otherwise disrupt the estate plans put in place through wills and trust instruments.[23]

### 2. Examine Transfer Restrictions

Many digital assets cannot be transferred during life or at death because terms of service agreements explicitly limit a user's rights to a limited, nontransferable license.

Apple's popular App Store, for example, subjects purchases to the condition that the purchaser "may not rent, lease, lend, sell, transfer redistribute [sic], or sublicense the Licensed Application and, if you sell your Mac Computer or iOS Device to a third party, you must remove the Licensed Application from the Mac Computer or iOS Device before doing so."[24] In other words, your iTunes account dies with you.

Even outright ownership of some digital assets, such as movies and music, may be subject to transfer and copy restrictions imposed by laws governing intellectual property, such as the Digital Millennium Copyright Act.[25]

For assets that can be transferred, some service providers are creating the ability for a user to make a transfer-on-death designation. Google, for example, has created an Inactive Account Manager service. With this service, a user may designate a person to be notified after an account has been inactive for a certain period. The user may also designate certain accounts to which the account manager may have access to download the contents.[26]

Such services, though few, are certainly catching the wave of the future to assist in the smooth administration of digital assets.

### 3. Appropriate Fiduciary Selection

Another consideration is who will be named as the fiduciary to marshal and manage the digital assets. Selecting a savvy fiduciary to handle assets with sentimental value (such as photos), actual value, or sensitive information (such as personal e-mail communications) can create a more efficient administration. It may also be appropriate to name a fiduciary to handle only these assets, if the other named persons would not be up to the task.

Planners may also consider incorporating specific authorizations in powers of attorney, revocable trusts and wills, or stand-alone documents to authorize disclosure under the CFAA or SCA. These authorizations may provide an alternative when state laws do not explicitly provide such authority to a fiduciary.

At present, however, these authorizations are riddled with problems, such as that a terms of service agreement may nullify the authorization. If such authorizations are used, consider carving out certain private information (such as certain e-mail accounts) that the authorized person may not access.

## Summary and Conclusion

Digital assets should be thoughtfully considered in estate planning and estate administration.

Fiduciaries should seek to identify a decedent's digital assets and the terms of service agreements that govern them. If transferable, these assets should be valued and reported on the estate tax return as well as in the probate filings.

Fiduciaries should also take care to consult with an expert before attempting to access digital assets, which attempt could expose the fiduciary to civil and criminal liability. Certain steps taken during a person's life to plan ahead for the transfer of digital assets, however, may significantly ease the administration of these assets in an estate.

Notes:

1. National Conference of Commissioners on Uniform Laws, Uniform Fiduciary Access to Digital Assets Act, Draft, June 6, 2014, at section 2, paragraph 9.
2. Id.
3. McAfee, "McAfee Reveals Average Internet User Has More Than $37,00 in Underprotected 'Digital Assets'," September 27, 2011, available at http://www.mcafee.com/us/about/news/2011/q3/20110927-01.aspx (accessed July 7, 2014).
4. Bitcoin Charts, http://bitcoincharts.com/markets/okcoinCNY.html (accessed July 7, 2014).
5. Karin Prangley, "Digital Life, Virtual Assets and Email," outline of materials presented at the 2013 Probate and Trust Law Section Conference, Minnesota Bar Association, June 11, 2013.
6. Id.
7. 18 U.S.C. § 1030 (2012).
8. Facebook Statement of Rights and Responsibilities, http://www.facebook.com/legal/terms (accessed July 7, 2014) ("You will not share your password . . ., let anyone else access your account, or do anything else that might jeopardize the security of your account.").
9. "Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. On Crime, Terrorism and Homeland Security of the H. Comm. On the Judiciary," 112th Cong. 112-80 (2011) (statement of Richard Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice).
10. Id.
11. See Tim Wu, "Fixing the Worst Law in Technology," *The New Yorker* (March 18, 2013), available at www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html.
12. Brian Fung. "The Justice Department used this law to pursue Aaron Swartz. Now it's open to reforming it." *Wash. Post* (February 7, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/07/the-justice-department-used-this-law-to-pursue-aaron-swartz-now-its-open-to-reforming-it/.
13. See WEC Carolina Energy Solutions LLC v. Miller, No. 0:10-CV-02775, CMC (4th Cir. July 26, 2012); U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012).
14. Nosal, 676 F.3d at 25.
15. 18 U.S.C. §§ 2701-2712 (2012)
16. 18 U.S.C. § 2702(b)(3) (2012).
17. In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things, No. C 12-80171 LHK, (N.D. Cal. Sept. 20, 2012).
18. National Conference of Commissioners on Uniform Laws, Uniform Fiduciary Access to Digital Assets Act, Draft, June 6, 2014.
19. Id. at section 7.
20. Id.
21. Id.
22. See PasswordBox, https://www.passwordbox.com/ (accessed July 1, 2014).
23. David Shulman, "Estate Planning for Your Digital Life, or, Why Legacy Locker is a Big Fat Lawsuit Waiting to Happen," S. Fal. Est. Plan. L. Blog (Mar. 21, 2009), available at http://sofloridaestateplanning.com/2009/03/articles/digital-assets/ (accessed July 1, 2014).
24. Apple, "Terms and Conditions" (September 18, 2013), available at http://www.apple.com/legal/internetservices/itunes/us/terms.html (accessed June 10, 2014).
25. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) (codified at various sections of Title 17 of the United States Code).
26. Google, About Inactive Account Manager, available at https://support.google.com/accounts/answer/3036546?hl=en (accessed July 1, 2014).

*Lauren G. Barron is an attorney in the Minneapolis, Minnesota, office of Faegre Baker Daniels LLP. Lauren's practice in the Wealth Management Group focuses on estate and tax planning and estate administration. Lauren can be reached at (612) 766-7558 or Lauren.Barron@FaegreBD.com.*

*Samantha L. Heaton is an attorney in the Minneapolis, Minnesota, office of Faegre Baker Daniels LLP. Samantha's practice in the Wealth Management Group focuses on estate and tax planning and estate administration. Samantha can be reached at (612) 766-8486 or Samantha.Heaton@FaegreBD.com.*

*Lauren and Samantha would like to thank Jonathan Nemani and Veronica Mason for their research assistance.*