Advisory

FEBRUARY 2014

PRIVATE CLIENT
SERVICES DEPARTMENT

ROBERT BENJAMIN
212.551.2602
rbenjamin@wiggin.com

KAREN CLUTE
203.498.4349
kclute@wiggin.com

MICHAEL CLEAR
203.363.7675
mclear@wiggin.com

DANIEL DANIELS
203.363.7665
ddaniels@wiggin.com

DAVID KESNER
203.498.4406
dkesner@wiggin.com

LEONARD LEADER
203.363.7602
lleader@wiggin.com

HELEN HEINTZ
203.363.7607
hheintz@wiggin.com

ARSINEH KAZAZIAN
212.551.2632
akazazian@wiggin.com

STEPHEN NAPIER
203.363.7659
snapier@wiggin.com

LISA PAGE
203.363.7635
lpage@wiggin.com

Estate Planning For Your Digital Assets

Each year an increasing number of people use social media technologies and assemble or acquire "digital assets" such as writings, pictures, videos and music in digital form. In most cases these assets do not have significant monetary value, but sometimes valuable intellectual property has been created. Regardless of economic value, many people attach a very high emotional value to their digital accounts and assets, but then fail to consider what will happen in the event of their death or incapacity.

This inattention can create confusion and distress for heirs. In cases involving valuable intellectual property, it can also result in economic loss. Without advance planning, families may be left to speculate about what their loved ones would have wanted done with their Facebook pages, personal e-mails, and computer files. Furthermore, unless express authorization has been given in advance, your heirs or executors may need to engage in litigation to access basic online accounts.

A few states have enacted laws that attempt to address the subject. For example, Connecticut and Rhode Island have enacted laws that require e-mail providers to give executors access to or copies of the contents of e-mail accounts that belonged to a decedent. While such statutes are sometimes criticized as being under-inclusive in the types of digital assets they provide for, they can be very useful. A user's e-mail account is often the single most important account that he or she has online. Many online accounts will send a copy of a user's login credentials to his or her e-mail account (or instructions on how to reset these credentials). Therefore, having access to an e-mail account can sometimes be like a "skeleton key" to some or all of a particular user's digital life. (For those people who do not want their executors to have such access, you should note that the Connecticut law does not have an "opt-out" provision.)

More typically, state law does not specifically address what happens to digital accounts and assets. (Legislation has been proposed, but not yet enacted, in New York.) In this situation, family members and fiduciaries must negotiate with service providers in order to gain access or control over digital accounts and assets. Depending on the service providers' terms of service and other contracts, this can be a nearly impossible fight to win. Newspaper reports of anguished families that have been unable to close social media accounts or access e-mails or other writings of a deceased loved one are an unfortunately common occurrence.

YOUR DIGITAL ESTATE

In thinking about what constitutes your "digital estate," you may want to account for two separate types of digital content: digital information and digital assets.

Digital information is comprised of items that were traditionally considered intangible personal property but can be managed online. Examples of digital information include online data concerning bank accounts and investment accounts.

CONTINUED ON NEXT PAGE

Estate Planning For Your Digital Assets CONTINUED

Even though digital information typically relates to property that is vital to an owner, issues involving access to digital information are not as common as with other types of digital property. Banks, brokers and creditors almost always have "offline" methods of dealing with the death or incapacity of a customer. Moreover, in the event of the owner's death, the underlying intangible assets represented by the digital information would pass to the owner's beneficiaries in accordance with traditional estate planning documents, such as wills, trust agreements and beneficiary designation forms. Thus, while it is recommended that digital information be stored and secured in the same way as traditional digital assets (discussed below), the failure to arrange for a way for your executor or heirs to have access to your digital information is unlikely to be catastrophic.

Digital assets include traditional digital assets that occupy physical space on a hard drive (e.g., photographs, music, family videos) as well as online accounts (e.g., social media pages, blogs, personal websites, e-mail accounts). Some online services are thought of as "dual-nature" assets because they contain characteristics of both traditional digital assets and online accounts (e.g., videos hosted on YouTube, pictures shared on Flickr, music files stored on iTunes, etc.). It is important to recognize that you may have digital assets that span across all of these categories, and to spend the time to identify and catalog them. You should also carefully consider who you would want to have access to these assets in the event of your incapacity or death, and who you would want to have ultimate control and ownership of these assets after your death.

SECURING AND BEQUEATHING TRADITIONAL DIGITAL ASSETS AND DUAL-NATURE ASSETS

As a general rule, the importance of an asset to an individual should correspond to the amount of redundancy used in storing that asset. Since traditional digital assets are static by definition, periodic backups to separate media should be conducted on a regular basis. The stored assets can then be secured, much like physical assets, and left with a fiduciary. For example, a backup of family pictures could be burned to a DVD or stored on a USB drive that is kept in a safe deposit box.

A similar strategy can be employed for dual-nature assets. These assets, by definition, are already stored by an online service, but redundancy can be achieved by storing copies of the assets on separate media. Securing dual nature assets in this manner also avoids the complexities surrounding giving access and control over online accounts, discussed below.

If you have traditional digital assets of great personal or economic value, you should consider specifically identifying such assets in your formal estate planning documents to ensure that they are properly administered in the event of your incapacity or death. Many traditional digital assets, unlike their physical counterparts, have the ability to be given to multiple parties. For example, a treasured family digital photo collection can be shared with virtually everyone. Conversely, the transmission of copyrightable original creative materials should be strictly controlled so as to preserve and manage the potential value of such assets.

CONTINUED ON NEXT PAGE

Estate Planning For Your Digital Assets CONTINUED

PLANNING FOR ONLINE ACCOUNTS

Online accounts are a relatively new form of property that is not addressed in the majority of states' probate laws. The ability to access saved account information, continue using an account, and terminate an account are all areas that are fraught with unsettled legal issues. Many online service providers (such as, for example, Yahoo! and Facebook) have provisions in their terms of service that forbid third party access to a member's account, and only provide access to executors or family members if ordered to do so by a court. Even if the requisite passwords are known, use of a password to access an online account without the authorization of the account owner can run afoul of computer privacy and fraud prevention statutes.

Given the uncertainty as to how online accounts will be handled in the event of the owner's death or incapacity, it is important to accurately document all of your online accounts and to communicate your wishes regarding the accounts. Even if you would just want your accounts to be deleted, you should consider how to make sure that a trusted family member or other person can access your online accounts. Due to the sensitive nature of sharing login credentials, several means of relaying this information might be considered:

- *Service Specific* – Some services have specific preferences that can be set by a user and then invoked automatically upon his or her death. For example, you may be able to have your account configured to automatically send saved e-mails to trusted contacts upon confirmation of your death. Other services have strict policies that will automatically delete a decedent's account upon proof of death, and will only grant access in response to a court order. Individuals should review the options that are available for their online accounts and determine if the terms of service are compatible with their wishes.

- *Digital Afterlife Company* – There are numerous online organizations that advertise services to store login credentials, messages, and files and to disseminate this information to trusted contacts upon the user's death. This may be a good solution, but there are serious risks that should also be considered. For example, the viability of a given service provider is not guaranteed. If a digital afterlife company goes out of business before your death, your stored information may be irretrievable. Also, by design, these services are hosted online and are therefore subject to online attack. If a hacker were to gain access to your account with the digital afterlife company, the damage could be considerable.

- *Password Sharing* – Computer security experts often counsel that sharing passwords is dangerous and can lead to unauthorized access and identity theft. Unfortunately, if a service-specific preference does not fit an individual's wishes, this may be the only possible option. In lieu of simply leaving a letter of instruction in a desk drawer, some advisors have suggested the following as ways of sharing passwords that can reduce the risks of unauthorized use.

  - *VAIL* – To use a Virtual Asset Instruction Letter or "VAIL," a person records all of his or her account data and corresponding login credentials in a physical letter that designates a fiduciary. The letter is then stored in a

safe deposit box and presented to the fiduciary upon the account owner's death. The problem with this approach is that login credentials can change, which would require the document to be repeatedly updated. In addition, while the information may provide the ability for an executor to access a decedent's account, the executor may still be in violation of the computer privacy and fraud prevention laws if the terms of service do not allow third-party access.

- *Two-Document Solution* – Another proposed solution is to use two separate letters: one that contains the account names and the other that contains the account passwords. The account owner then provides each letter to a separate individual and instructs each of them not to combine the information until after the owner's death. The objective of this approach is to prevent an individual from misusing information provided by a VAIL or other means before death. This is a problematic solution, however, because the two individuals could decide to not share their information for any number of reasons. In addition, this solution is not as balanced as it may seem. The username for many online services can be obtained with little effort and often stays the same between various accounts. (This is especially true of e-mail accounts.) Therefore, the holder of the password letter could be accused of unauthorized access, which would defeat the purpose of the system.

- *Will/Trust Incorporation* – Login credentials for online accounts should not be recorded in a will, because when the will becomes part of the public record, it would open up the door for unauthorized access. Some advisors have proposed using a revocable trust, which is a private document, instead. The idea is that the owner, as trustee, would register the online accounts in the name of the revocable trust so that, in the event of the owner-trustee's incapacity or death, control of the account would pass to a successor trustee. In theory, this approach should make transferring online account credentials both seamless and secure, but it would most likely involve creating a separate revocable trust for this sole purpose and may be practical only for owners with very valuable digital assets.

- *Data Recovery* – If a decedent dies without planning for his or her digital estate, all might not be lost. Data forensic examiners and recovery specialists can be hired to salvage login credentials and some types of protected files from the decedent's hard drive. But this method should only be used as a last resort. Data recovery services are expensive, can end up retrieving unreliable information, and may recover information that the decedent intended to keep confidential and/or have destroyed.

For many clients, planning for their digital assets should be an important part of their overall estate plan. For personalized advice relating to how your digital assets fit into your estate plan, please contact your Wiggin and Dana attorney.

ABOUT THE PRIVATE CLIENT SERVICES DEPARTMENT

Our experienced and highly skilled Private Client Services attorneys help our varied clients, both national and international, and from wide-ranging businesses and professions, deal successfully with complex issues that impact them and their families.