KENDAL R. DOBRA

Riding the Digital Wave:

An Executor's Fiduciary Duty toward Digital Assets

Meet Lauren Elizabeth. Lauren is an avid blogger of fashion and style, and her blog boasts over 3,000 subscribers.[1] In addition to producing multiple blog entries per week, Lauren offers virtual styling services: for a set hourly rate she will, via online video chat, assist you in cleaning out your closet, developing a new personal wardrobe or any other styling service by request.[2] She will bill you exclusively using PayPal.[3] Lauren also generates blog related revenue by offering advertisement space on her webpage,[4] and she also provides a link to her Etsy shop where online customers can purchase her handcrafted jewelry.[5] In addition to her blog, Lauren, her mother, and her sister offer an e-cookbook available for a set price per download.[6] Lauren has essentially created a source of income solely by producing and marketing digital assets. What would happen to Lauren's blog if she was to pass away without properly addressing her digital assets and accounts in her estate plan? What if there were outstanding invoices for her styling services or uncollected advertisement revenue? How would Lauren's family collect that income? Who would decide what would happen to Lauren's blog content and domain name? Lauren is merely one example of the millions of bloggers flocking to the Internet in search of a supplemental or primary income stream.

Digital assets can have substantial value. Blogs and domain names have sold for millions of dollars,[7] and fortunes have been generated solely through the participation in virtual games such as Second Life.[8] Individuals use the Internet as a medium to keep in touch with family and friends, store information, pay bills, share photographs, and for countless other uses.[9] The primary form of modern communication is email, not handwritten letters or phone calls.[10] Assets

that were once discoverable by looking through a person's papers or filing cabinet can now exist solely in cyberspace.[11]

How should fiduciaries deal with the unrelenting onslaught of digital assets? How should an executor handle digital assets when settling an estate where the estate plan did not contemplate them? This article discusses exclusively an executor's duty toward digital assets, but it is worth mentioning that all fiduciaries, such as conservators, agents, and trustees, also face challenges when dealing with digital assets.

Executors have a duty towards digital assets, be it to administer or merely protect them, and this article explores how an executor should satisfy this duty and the potential impediments to doing so. Part I explains what digital assets are and how they are accessed. Specific types of digital assets are examined further in Part II where the value of the various digital assets is discussed. Part III addresses the problems faced by executors when dealing with digital assets, and Part IV explores the legislative solutions that have been offered to address those issues. The article concludes in Part V with proposed methods for satisfying an executor's duty toward digital assets.

I. What Are Digital Assets?

One of the difficulties in managing or even discussing this topic is that there is not a universal definition of "digital assets."[12] Contributing to that problem is the fact that digital assets themselves are in a state of constant evolution, morphing to meet the new demands and innovations of the Internet.[13] People are creating digital assets with button clicks or keyboard strokes, possibly without even realizing that they could be creating property. Email, social media accounts, blogs, and even some virtual games have the potential to be deemed property.[14]

The most recent draft of the Fiduciary Access to Digital Assets Act being drafted by the Uniform Law Commission goes further than offering a singular definition of digital assets. It distinguishes between digital assets and digital accounts.[15]

> "Digital account" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information which provides access to a digital asset or a digital service. "Digital asset" means information created, generated, sent, communicated, received, or stored by electronic means on a digital service or digital device; the term includes a username, word, character, code, or contract right under the terms of service agreement.[16]

The distinction between a digital account and a digital asset becomes important when dealing with access to property versus access to accounts. An executor may be given access to content created by the decedent that is held in an account more willingly than she would be given continuous access to manage the email account itself.[17]

Regardless of the precise definition, experts agree that digital assets are, at minimum, information stored in an intangible medium on computers or other computer related technology.[18] Digital assets are accessed through a tangible piece of property such as a computer, hard drive, smartphone, or third party server.[19] If they are stored online, they often require a password in order to be accessed.[20] They can be classified into four categories that will be explored more thoroughly in Part II: personal, social media, financial, and business.[21]

II. Are Digital Assets Valuable?

Digital assets have both monetary and sentimental value. Internet users in the United States are estimated to own approximately $55,000 worth of digital assets per user.[22] In addition their monetary value, digital assets such as pictures and videos represent significant sentimental value to the loved ones of a decedent.[23] The potential value of digital assets is being recognized by estate planners,[24] and they are beginning to offer clients advice regarding how to plan for disposition of these digital assets.[25]

a. Personal Digital Assets

Personal digital assets are digital assets that primarily have sentimental value.[26] They consist of digital photographs, digital videos and email correspondence to name a few examples.[27] Traditionally, photo albums and letters were stored in boxes in closets, but technology has transformed them from their traditional physical form to an intangible medium.[28] Users create free online email accounts with companies such as Google and Hotmail, and use those accounts for any range of correspondence – personal and business. Users often receive banking statements, notification of online subscriptions, and notifications of pending sales in online auction houses only through their email accounts.[29] While the monetary value of personal digital assets are usually less than an individual's other more liquid assets, the sentimental value of those same assets will be priceless to a decedent's family.[30] Additionally, much like a decedent's physical mail, email can provide valuable information to an executor such as: notice of outstanding debt, notification of financial accounts and other insights into a decedent's life.[31]

b. Social Media Assets

Social media accounts like Facebook and Twitter are growing exponentially. As of May 7, 2013, Twitter has 554,750,000 active registered users worldwide, and the number is estimated to grow by 135,000 daily.[32] Like personal digital assets, the monetary value of one's social media accounts will be nominal at best. The exchange of information or storage of other digital assets found in social media accounts may become paramount to the families of a decedent.[33] Information stored in their Facebook messages or pictures can provide families with a glimpse into their loved one's life that may be unavailable in any other method.[34] Pictures and memories could be lost forever through callous deactivation of these accounts.[35]

c. Financial Accounts

Financial accounts also come in various forms. They include accounts where money is exchanged online such as online bill payments or other financial accounts designed only to operate online.[36] Banks now exist that operate exclusively online.[37] Online transfer services, such as PayPal, provide users with a venue to transfer funds from one individual to another without writing a check or swiping a debit card.[38] PayPal alone has 128 million active accounts and facilitates approximately $7.8 million in transfers daily.[39] Online currencies also represent a new form of financial digital assets.[40] Bitcoins, for example, are an exclusively online currency that are generated by solving a complex math equation that requires an immense amount of computer power to calculate.[41] They are acquired through creation or are purchased through online exchanges.[42] Although bitcoins are reportedly being used by individuals who primarily use the currency for illegal online purchases,[43] the overall value of all bitcoins being traded is estimated to be above $1 billion,[44] and bitcoins represent only one of the online currencies available. Financial assets also come in the form computer accounting programs, such as TurboTax and Quicken that are designed to make it easier for individuals to store personal financial records solely on their computer. [45] These types of files are necessary to administer an estate and can provide valuable insight into a decedent's overall assets, especially in a case where the decedent did not keep hard copies of records.[46]

d. Business Accounts

Perhaps one of the fastest growing subsets of digital assets is business accounts. Traditional businesses are flocking to the Internet to meet the public's expectation that they have a web presence, and they are innovating ways to facilitate web interaction with customers.[47] A business may have more than one user authorized to access its digital business accounts located

either online or on its internal computer system; however, what if your decedent operated a small business such as a blog and/or she is the only person who has access to that digital asset?

Blogs offer individuals a medium to project their opinions and advice to the world via the Internet through daily entries on specific topics. While blogs could be classified as personal assets akin to a diary, blogs can also generate a steady revenue stream.[48] A high number of blogs exist with one website provider boasting over 66 million websites.[49] Blogs have two distinct property interests belonging to the blogger: the copyrightable content and the domain name.[50]

Bloggers can use blogs to produce earnings in a variety of ways.[51] They can sell ad space on their page or incorporate product promotions into their blog entries; or bloggers can create an eBook out of their most popular blog entries.[52] In extreme circumstances, they may even be able to market their blog content into a movie or book.[53] The movie *Julie & Julia* chronicled a woman's experience of cooking through Julia Child's cookbook and blogging about her experiences, and it grossed over $129 million.[54] However, the value of the blog is often directly related to the blog's followers and content generated by the blogger, so when the blogger passes away, it is likely their blog will no longer have substantial monetary value. That being said, outstanding revenues may need to be collected or the family of a decedent may try to market the blog content. The blogger's content will have at least sentimental value for family and friends.[55]

Regardless of the content value, the domain names will have a separate, distinct value.[56] Domain names can become inactive if they are not renewed, and when they are inactive for up to 12 months, they can be recycled and resold without notification or the knowledge of the original owner.[57] Domain names likely have nominal value, but they could represent a significant asset of a decedent. Sex.com, for example, reportedly sold for $13,000,000 in 2010, and fund.com reportedly sold for $9,999,950 in 2008.[58]

III. Problems Executors Face Today

Someone well acquainted with the duties of an executor might logically assume that an executor has the right to access all of the decedent's assets, but, in fact, an executor faces a plethora of challenges when accessing digital assets.[59] Even when an executor takes possession of a decedent's tangible technology devices, they still face the challenge of accessing the stored digital assets if the tangible device is protected by a password or if the files themselves are encrypted.[60] A common solution presented by estate planners is for individuals to leave behind a list of digital assets and the associated passwords with instructions that their executors and/or loved ones use the information to access their digital assets and accounts.[61] Furthermore, password-saving services have even emerged to facilitate the terms of transfer of those passwords at death.[62] Even with the decedent's "authorization and putting aside other criticisms of this practice, accessing a decedent's digital assets through the use of their existing passwords could potentially violate federal law.[63]

a. The Potential Criminal Liability under the Computer Fraud and Abuse Act

One impediment to accessing digital assets is the Computer Fraud and Abuse Act ("CFAA").[64] The CFAA states that "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer" will be punishable either by a fine or potentially imprisonment.[65] The potential for an executor's violation of the CFAA centers around whether or not violation of a website's Terms of Services Agreement ("TOSA") indeed violates the "without authorized access or exceeds authorized access" portion of the CFAA.[66] TOSAs sometimes state that no one but the registered user is authorized to access the digital asset,[67] and courts have held that a mere violation of a

website's TOSA account can be a violation of the CFAA.[68] However, the interpretation and applicability of the CFAA varies and is still being solidified.[69]

The CFAA contains no specific exemption or authorization for executors attempting to access a decedent's digital assets.[70] Proposed revisions to the CFAA have been rebuffed by the Department of Justice whose representatives have gone on record as interpreting the CFAA to "permit[s] the government to charge a person with violating the CFAA when that person has exceeded his access by violating the access rules put in place by the computer owner and then commits fraud or obtains information."[71] Consequently, it is foreseeable that an executor could face criminal liability under the CFAA simply by using a decedent's passwords or by accessing a decedent's computer files,[72] presenting a potentially huge impediment to fiduciary access to digital assets.

b. The Stored Communications Act

The Stored Communications Act (the "SCA") protects the privacy interest of a user's stored communications by forbidding access by unauthorized users.[73] However, service providers may give access to unauthorized users if one of the eight explicitly listed exceptions applies.[74] That being said, the SCA , like the CFAA, does not specifically provide for or deny fiduciary access to the stored communications.[75]

An executor could also be criminally liable for utilizing a decedent's password under the SCA as well. Adding to the uncertainty surrounding "unauthorized access" in the SCA, a jury recently awarded $450,000 in damages for unauthorized access of a user's email account.[76] In *Cheng v. Romo,* a physician gave his co-worker his password to his personal email account with the implied understanding that the co-worker would use it for a limited, business purpose.[77] Years later, the co-worker accessed the physician's email using the password for an

uncontemplated use, and the physician sued for damages.[78] The jury's damage award seems to confirm that the determination of whether or not access is authorized or unauthorized is fact specific.[79] Executors who utilize passwords that have been left behind by a decedent could be liable for damages if their use is deemed "unauthorized."[80] Contrastingly, it is also possible that when a decedent leaves their passwords in conjunction with express permission for an executor to use them, it may be seen as "authorized access" under both the SCA and the CFAA.

The relationship between a service provider's adherence to the SCA and an executor's access to a decedent's digital assets where passwords were not left behind was tentatively explored in *In re Facebook*.[81] A family of a decedent approached Facebook for access to the decedent's account in order to gain a better understanding of the decedent's apparent suicide.[82] Facebook successfully quashed a civil subpoena initially granted to provide access to the decedent's account on the grounds that it violated the SCA.[83] The court held that in order to uphold the privacy protections instilled by the SCA on service providers, civil subpoenas in general may not compel providers like Facebook to produce the records of a decedent.[84] The court was careful to point out that its ruling did not prevent Facebook from willingly revealing the records, an action permitted by the SCA.[85] The court suggested that Facebook could choose whether or not the decedent's family had standing to "authorize" access on the decedent's behalf, but then declined jurisdiction over the issue.[86] The ambiguity surrounding the interpretation of the SCA has arguably led to a variety of fiduciary access policies among service providers.[87]

IV. Legislation Addressing Digital Assets

a. Existing State Legislation

Some states have recognized the growing problem of a fiduciary's lack of access to digital assets and have directly addressed the issue via state statutes.[88] The statutes can be

divided into three generations seemingly based on the technology available at the time of enactment.[89] California, Connecticut, and Rhode Island were the first states to address the issue, and all three statutes focus exclusively on a fiduciary's access to email accounts.[90] Indiana followed, but extended the access to include records stored electronically.[91] The third generation of state statutes are being proposed at the writing of this article, and they take into consideration social networking sites.[92] While the statutes are progressive, one criticism is that most do not address future technological developments that will inevitably occur.[93]

b. Proposed Uniform Fiduciary Access to Digital Asset Statute

The Uniform Law Commission is attempting to clarify of the ambiguities of the CFAA and the SCA. It has created a committee tasked with drafting a Uniform Fiduciary Access to Digital Asset Act (the "Act"). Its goal is to "vest fiduciaries with at least the authority to manage and distribute digital assets, copy or delete digital assets, and access digital assets."[94] The Act will not be finalized until 2014, but the current draft may solve at least one of the major hurdles currently faced by fiduciaries under the CFAA and the SCA by explicitly stating that a fiduciary has the requisite "authorized access" under both of those federal statutes.[95] If adopted uniformly, the Act promises to clear current ambiguities with respect to digital assets. That being said, the committee still faces the challenges of finalizing the Act and its subsequent uniform adoption by the 50 states. Also, the "authorized access" issues arising under the CFFA and the SCA are issues of federal law, and the Act proposes to alter state law.[96]

V. How Does Today's Executor Ride the Digital Wave?

An executor is charged with the responsibility of settling a decedent's estate which entails discovering, protecting, and facilitating the transfer of all of the decedent's property.[97] To that end, it is not uncommon for an executor to physically go through a decedent's file cabinet,

records, safe deposit box, or even the deceased's personal effects. [98] In some cases, an executor might forward a decedent's mail to her office.

Executors are responsible for taking reasonably necessary steps to administer an estate.[99] Generally, if a decedent had the right to do something with his or her property an executor has that right as well,[100] but how do these duties translate to the digital world? If there are reasonable steps available to an executor to ascertain whether or not a decedent has digital assets or if it is established that a decedent does have digital assets, an executor is obligated to take those steps reasonably necessary to discover and marshal those assets in an effort to administer an estate.[101] If the executor does not take these steps, she risks breeching her fiduciary duty.[102] The estate administration of digital assets may be made easier if a decedent contemplated digital assets in their estate plan,[103] but even if digital assets were not contemplated, it is necessary for an executor to seek them out.

The following is an accumulation of suggested methods that would be reasonable for an executor to exhaust while settling an estate. They would aid in reducing the potential liability an executor could face for not performing her duty towards digital assets. The intent is not to create an exhaustive list of solutions; rather, it is meant to illustrate the reasonableness and simplicity of the steps an executor can take to avoid potential liability.

a. Step One: Marshal the Assets

An executor has the duty to marshal all of a decedent's assets in order to facilitate the transfer of those assets in accordance with the decedent's wishes or state intestacy laws.[104] The duty to marshal extends to all the property owned by a decedent.[105] Where applicable, an executor should include all assets of an estate on the decedent's estate tax return including digital and non–digital assets.[106] If an executor does not marshal all of the assets of the estate, they risk

filing an incomplete inventory or estate tax return or losing the value of the asset all together. Non inclusion of the asset on an estate tax return could result in the executor being liable for penalties or fees associated with not reporting the asset.

Another consequence of not marshalling a decedent's digital assets is that the assets could be lost to the beneficiaries.[107] For example, funds remaining in a PayPal account that has remained inactive for a period of two years will first be forwarded to the owner's indicated primary address, and, if necessary, will be escheated to the state of their primary address.[108] Even in an instance where the digital asset does not have a monetary value, the digital asset may have significant sentimental value to a decedent's loved ones.[109] Individuals are recording their lives online via their personal or social media digital assets and accounts instead of through traditional non-digital mediums.[110] If these assets are ignored by an executor, the decedent's life story could be lost to their loved ones.[111]

Digital assets play an important role during an individual's lifetime, and can be a significant part of a decedent's estate. They should not be allowed to disappear simply because they have not been marshaled by an executor. The following explores several methods available to an executor to marshal digital assets.

i. Secure Physical Technology Devices Owned by a Decedent

Computers and other various tangible technology devices serve as portals to and storage of digital assets.[112] Files that include written works or pictures and computer programs are loaded directly on the computer hard drive, and passwords to online accounts can be saved automatically through the Internet browser.[113] However, due to various security measures, an executor may not have the skills to even access the computer itself; consequently, an executor may have to hire a computer expert to essentially "break-in" to the computer.[114]

Once a computer is accessed, the executor can look through the computer's files and programs to ascertain what digital assets are present on the hard drive and to determine if those assets are valuable – be it sentimental or monetarily.[115] Next, the executor should look through the browser history, favorites, or bookmarks in the Internet browser to determine if the decedent had an online presence.[116] An executor may be able to access a decedent's digital assets by utilizing the saved passwords in the browser, but an executor should keep in mind that accessing an online account for which the executor is not the owner could violate the website's TOSA and may be a punishable offense under the CFAA.[117]

ii. Google the Decedent

Substantial information regarding a decedent could be gleaned by entering the decedent's name into one of several Internet search engines. The search may not be revealing because of the anonymity of the Internet, but this represents a reasonable, simple step that an executor could take in attempting to discover online digital assets such as a blog or registered domain name. Additionally, an executor can search various free search engines for domain names by searching for the decedent's computer's Internet protocol address to determine if the decedent owned any domain names. [118] If an executor has reason to suspect a decedent did own a domain name, but free searches have not revealed the asset then an executor should take the additional step of hiring a professional search service, such as DomainTools, for a fee.[119]

By not conducting thorough searches for digital assets, an executor can open themselves up to liability for not exercising reasonable care in marshalling a decedent's assets. An executor who unknowingly allowed a domain name such as "sex.com" to be recycled and sold by the registry rather than by the decedent's estate will likely face extremely unhappy beneficiaries, not to mention liability for not reporting assets on an estate tax return.

iii. Analyze Bank Statements & Paper Records

Just because a decedent has digital assets does not mean that they have not left a paper trail of those digital assets.[120] A decedent's bank or credit card statements might show regular charges for a domain name or an online storage facility, or they might reveal transfers between a PayPal account or a Bitcoin exchange.[121] An executor should always be on the lookout for signals that a decedent may have had digital assets or digital accounts.

iv. Search E-Mails

Emails can be a useful tool for marshalling digital assets.[122] They can reveal the existence of various digital assets such as banking accounts, web subscriptions, or even bill payment accounts.[123] Considering the amount of emails one account might contain, a computer program could be used to electronically search the emails for keywords or by sender. One of the primary roadblocks to executing this step is the potential for email service providers to deny fiduciaries in general access to the decedent's content and account.[124] This possibility is more thoroughly explored later in this article.

Accessing a decedent's personal email account presents one set of issues; accessing a decedent's employer-provided email accounts presents additional issues. [125] In addition to the protections invoked by email service providers, the decedent's employer may refuse access claiming the protection of trade secrets or policy violations, adding another layer of resistance an executor might face.[126] Even with the potential for the decedent's employer to deny an executor access, an executor should still request the decedent's email contents as they could contain valuable information regarding the decedent's assets.

v. Deactivate Social Media Accounts

An executor should discover whether or not a decedent had a social media presence. Once ascertained, the decedent's family may be interested in obtaining the content stored in those accounts whereby the executor should attempt to gain access to them. At minimum, an executor should contact those social media sites to notify them of the death, and the social media site will take the step outlined in their respective TOSA. Facebook, for instance, will memorialize a user's page essentially freezing it as a shrine to the decedent.[127] Also, an executor should be aware of whether or not the decedent had other online accounts such as dating services like Match.com. The executor should in turn contact those sites and notify them of the decedent's passing.

b. Step Two: Possess Digital Assets

Once the assets have been marshaled, an executor should take into their possession all of the assets of an estate that are necessary for the administration of the estate, including digital assets.[128] The following offers suggested methods of an executor could take when attempting to posses digital assets that are, by definition, intangible.

i. Determine if the Digital Asset is Property

Once the assets are marshaled, the first thing an executor should determine is whether or not the digital asset discovered is indeed an asset that was able to be owned and transferred by the decedent. Individuals might assume they have an unlimited property right in their email accounts when, in reality, the user might only have a right to access those assets during life and the right to those assets terminates at their death.[129] A Yahoo! email address is non-transferrable and will be de-activated upon notice to Yahoo! of a user's passing.[130]

Music files might also be assumed to be the transferable property of a decedent, but that is not always the case. For instance, a popular application for downloading entertainment files is iTunes.[131] Individuals spend enormous amounts of money over their lifetimes purchasing files for their iTunes account, so a decedent's iTunes account could potentially represent a substantial asset.[132] Nevertheless, in accordance with iTunes TOSA, files downloaded during a user's lifetime are nontransferable at their death.[133] Consequently, the TOSA associated with each asset should be examined to determine if the user is granted a property interest, and, if a property interest is granted, to what extent is the interest transferable.

ii. Use Your State's Access to Digital Asset Statute

Previously discussed in this article were several existing and proposed state statutes that specifically address a fiduciary's access to certain digital assets. If the state where an estate is being settled has a statute that allows the executor to obtain access to digital assets and if an executor deems that a decedent has or may have digital assets, the executor is under an obligation to utilize that statute to its full extent. The reasonableness of this step depends directly on the state in which the estate is being settled.

iii. Ask the Service Provider for Access to Stored Digital Assets

Once an executor discovers that digital assets exist and determines that further exploration of those assets is warranted, an executor should ask the service provider for access to the stored digital assets[134] – a deceptively simple task. Service providers are generally reluctant to provide an executor with access to a decedent's stored communications; hence, an industry standard for fiduciary access to digital assets does not exist.[135]

Service providers have unique accessing procedures for stored digital assets.[136] Email providers such as Hotmail and Google each provide separate procedures for accessing a

decedent's emails.[137] Yahoo! on the other hand, will not provide information or access to the decedent's account; rather, it will deactivate the account immediately upon proper notification of the user's death.[138] Storage providers such as Dropbox will give an executor access to a decedent's stored files if the executors provide Dropbox with the necessary documentation.[139] In contrast, users of iCloud will lose stored information forever upon passing.[140] Consequently, an executor should be familiar with the TOSA of the digital account they are attempting to access.

vi. Petition a Court for Access to the Digital Assets

If a service provider refuses to provide an executor with access to digital assets upon request, it might be necessary for the executor to seek a court order compelling the service provider to reveal the information.[141] Depending on a family's wishes and potential of discovery, an executor may not need to take this step. The success of these types of actions has varied, but there is one common theme throughout the cases.[142] In each instance, the families of the decedent were aware that digital assets existed and actively sought possession of those assets.[143] An executor should balance the wishes of the heirs of the estate with the potential cost of litigation for the release of the digital assets to determine if this step is reasonable. The specific circumstances are essential to making the determination.

v. Use Passwords Left Behind

Estate planners are advising clients to leave a list of their passwords behind in some medium.[144] If a decedent does leave a list of digital assets and accounts with the associated passwords and the express permission that an executor may use them, then it is reasonable to expect an executor to use them.[145] Again, an executor should be wary of the potential violation of the SCA[146] or the CFAA.[147] As previously discussed, it is uncertain whether or not using the decedent's left-behind passwords constitutes authorized access under the federal laws.[148] Some

advocate password use based on the premise that an executor steps into the shoes of a decedent and thereby has the authority to access digital assets,[149] but that view is not solidified law. An executor has to circumstantially assess for herself whether accessing those assets is worth the risk of the potential for criminal liability.

c. Step Three: Protect the Estate

An executor may take all steps reasonably necessary to protect and preserve the estate.[150] In addition to traditional concerns when administering an estate, the presence of digital assets raises various new concerns such as the identity theft of a decedent or the monitoring of copyrighted material.

i. Delete Files from Tangible Digital Property

A computer and other hard technology devices would be considered tangible personal property under a decedent's will, assuming the decedent has a will; therefore, they will pass as the decedent directs their tangible personal property to be disposed.[151] Often a decedent will direct their tangible personal property pass to a relative or friend. However, prior to an executor delivering these assets, an executor should consider wiping the computer files and browsing history of the technology device in an effort to protect the estate.[152]

As previously mentioned, an Internet browser has the capability to retain user names and passwords for various online accessible accounts such as banking accounts, email accounts, or social media accounts. If the device is passed to an individual without clearing the device of these portals to digital accounts then the executor takes the risk that a decedent's various online accounts could be accessed by an unauthorized third party.[153] Contrastingly, by deleting files from a technology device, an executor may be irrevocably destroying assets that the decedent's

heirs would traditionally be able to access if the assets existed in a non-digital form such as family photographs or personal correspondence.[154]

An executor should weigh their duty to the estate's beneficiaries and their duty to the estate, and, based on that assessment, should determine their course of action. If a cursory search of a decedent's computer reveals only that they utilized the Internet for online bill pay features and if they only stored photographs on their computer's hard drive, it is reasonable for an executor to pass the computer to the intended heir after clearing the browsing history and passwords potentially stored by the Internet browser. Conversely, a more thorough examination of a decedent's stored digital assets would be warranted if the decedent was an avid computer user. They may have encrypted files, tax information or other various digital assets saved to the hard drive that should be extracted and the hard drive wiped clean.

ii. Notify Credit Agencies of the Decedent's Death

Identity theft of deceased individual's identities is a frequent occurrence, with a reported 800,000 of deceased Americans' identities intentionally targeted annually.[155] In addition to the fraudulent applications for credit and services, an increasingly popular use of stolen identities is the filing of fraudulent tax returns and the subsequent collection of the refund.[156] Any one of the many uses of a stolen identity could delay the settlement of the estate. The estate would also incur additional executor fees representative of the time she would have to spend remedying the issues arising from the fraud duplication.

Various methods exist for protecting against identity theft. One recommendation is to vigilantly monitor banking accounts and credit reports;[157] however, an executor may not have the ability to monitor certain accounts that are accessible only online. Another recommendation is to reach out the credit reporting agencies to notify them of the decedent's death and to put a freeze

on the decedent's social security number.[158] Each of the credit reporting agencies will accept notification of a decedent's death from the executor of the estate and will place a death notice on the decedent's file, and at least one will place a seven year promotional block on the deceased accounts. [159] Although each agency has slightly varying requirements for notification, the notification can generally be completed with a simple letter and proof of executor appointment.[160]

An executor has the duty to protect the assets of the estate, which extends to protecting the deceased's identity. Dealing with a decedent's stolen identity could prolong the settlement of the estate and unnecessarily increase the executor fees charged the estate. Executors can hedge against the potential of identity theft by taking the simple step of notifying the credit reporting agencies of a decedent's death.

iii. Protect Copyrighted Digital Assets

If an executor discovers that the decedent had a copyrighted digital content displayed online, such as a blog or photographs, an executor should take necessary steps to protect those assets from copyright infringement. If possible, an executor should remove the copyrighted material from the purview of the public so as to minimize the chance of copyright infringement. Also, they should be aware of potential copyright infringing uses of the decedent's works.[161] If an infringing use is found, the executor should take the necessary steps to report the infringement pursuant the provisions outlined in the Digital Millennium Copyright Act of 1998; however, an executor may face unique challenges in filing this claim stemming from the fact that the executor themselves do not own the copyright.[162] The possibility of failure does not preclude an executor from attempting to protect the work.

Conclusion

Digital assets are the wave of the future as evidenced by their continuing exponential development, and executors can no longer afford to assume that a decedent does not have an online presence. An executor has the duty to seek out digital assets, possess those with value, and distribute them in the same manner non-digital assets have been administered for decades. Proper planning and contemplation of digital assets and accounts in an estate plan will help an executor successfully administer an estate, but an executor cannot rely on proper planning alone. She has the duty to seek out and administer digital assets and faces the potential to be held liable for not exhausting reasonable methods to satisfy that duty.

[1]*See generally* Lauren Elizabeth, THE LAUREN ELIZABETH, http://www.thelaurenelizabeth.com (last visited June 3, 2013).
[2] Lauren Elizabeth, *Services*, THE LAUREN ELIZABETH, http://www.thelaurenelizabeth.com/p/hire-me.html (last visited June 3, 2013).
[3] *Id*.
[4]Lauren Elizabeth, *Advertise,* THE LAUREN ELIZABETH, http://www.thelaurenelizabeth.com/p/sponsor.html (last visited June 3, 2013).
[5] *See* Elizabeth, *supra* note 1.
[6] Kate, *Three Ruffled Aprons: an eCookbook!*, The Small Things Blog (Dec. 6, 2012), http://www.thesmallthingsblog.com/2012/12/three-ruffled-aprons-ecookbook.html.
[7] Jeff Bercovici, *AOL Buys the Huffington Post for $315* Million, FORBES (Feb. 7, 2011, 12:38 AM), http://www.forbes.com/sites/jeffbercovici/2011/02/07/aol-buys-the-huffington-post-for-315-million/.
[8] Rob Hof, *Second Life's First Millionaire*, BLOOMBERG BUS.WK. (Nov. 26, 2006), http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_fi.html.
[9] Victoria D. Blachly & Michael Walker, *Virtual Assets,* ST003 A.L.I-A.B.A. 175, 177 (2011).
[10] *Id.*
[11] Colin Korzec & Ethan A. McKittrick, *Estate Administration in Cyberspace*, TRUSTS & ESTATES, Sept. 2011, at 61, 61.
[12] Gerry W Beyer, *Estate Planning in the Digital Age*, 1 (Apr. 21, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166422.
[13] *See* Jamie B. Hopkins, *Afterlife in the Cloud: Managing a Digital Estate*, 5Hastings Sci. & Tech. L.J. 210, 211-12 (Summer 2013).
[14] Korzec & McKittrick, *supra* note 11, at 62.
[15] *See Draft Fiduciary Access to Digital Assets,* NAT'L CONF. OF COMM'RS. OF UNIF. STATE LAWS, 3 (Feb. 2013), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013feb7_FADA_MtgDraft_Styled.pdf.
[16] *Id.*
[17] *See* Gerry W. Beyer & Naomi Cahn, *Digital Planning: The Future of Elder Law*, 9 NAELA J. 135, 141 (2013).
[18] Hopkins, *supra* note 13, at 211.
[19] *See id.* at 212.
[20] *Id*.
[21] Beyer & Cahn, *supra* note 17, at 137.
[22] *McAfee Reveals Average Internet User Has More Than $37,000 in Underprotected Digital Assets,* MCAFEE (Sept. 2011), http://www.mcafee.com/us/about/news/2011/q3/20110927-01.aspx (asserting that users are unaware of the value of their digital property).
[23] Beyer & Cahn, *supra* note 17, at 140.
[24] Gerry W. Beyer & Naomi Cahn, *When you Pass On, Don't Leave the Passwords Behind*, 26 PROB. & PROB. 40, 41 (2012).
[25] *Id*.
[26] *See* Beyer & Cahn, *supra* note 17, at 138 (describing various personal digital assets).
[27] *Id*.
[28] Hopkins, *supra* note 13, at 217.

[29] James D. Lamm, Remarks at the Annual Heckerling Inst. on Est. Plan., *Digital Death: What to Do When Your Client Is Six Feet Under, But His Data Is in the Cloud*, 35 (Jan. 17, 2013) (outline available by contacting author at James.Lamm@gpmlaw.com).
[30] *See* Beyer & Cahn, *supra* note 17, at 137.
[31] Lamm, *supra* note 29, at 35.
[32]*Twitter Statistics,* STATISTIC BRAIN (May 7, 2013) http://www.statisticbrain.com/twitter-statistics/ (stating that Twitter has 554,750,000 active registered users with 135,000 new users signing up daily).
[33] *See* Maria Perrone, Note, *What Happens When We Die: Estate Planning of Digital Assets*, 21COMMLAW CONSPECTUS 185, 196-99 (2012/2013) (summarizing cases where loved ones sought content preserved on social media accounts).
[34] *Id*.
[35] *See id*.
[36] Beyer & Cahn, *supra* note 17, at 138.
[37] *See generally* ALLY BANK, http://www.ally.com (last visited June 6, 2013) (illustrating that Ally Bank operates exclusively online to the extent cash deposits are not accepted).
[38]*About PayPal*, PAYPAL, https://www.paypal-media.com/about (last visited June 6, 2013) (describing PayPal's services and the extent to which they are used).
[39] *Id.*
[40] Richard Satran, *How Did Bitcoin Become a Real Currency?*, U.S. NEWS (May 15, 2013), http://money.usnews.com/money/personal-finance/articles/2013/05/15/how-did-bitcoin-become-a-real-currency (discussing the creation and use of bitcoins).
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] Lamm, *supra* note 29, at 37.
[46] *Id.*
[47] Hopkins, *supra* note 13, at 214-15.
[48] *See, e.g* Elizabeth, *supra* note 1.
[49] *WordPress Sites in the World*,WORDPRESS, http://en.wordpress.com/stats / (last visited June 6, 2013) (stating number of websites provided through WordPress worldwide).
[50] Lamm, *supra* note 29, at 55.
[51] Amrik Virdi, *The Secret of How to Make Money Blogging,* BASIC BLOG TIPS (Feb. 11, 2013) http://basicblogtips.com/make-money-blogging-secret.html.
[52] *Id.*
[53] *See* Lamm, *supra* note 29, at 56.
[54] *Id.*
[55] *See* Perrone, *supra* note 33, at 196-99.
[56] Lamm, *supra* note 29, at 56.
[57] *What Happens if my Protected Domain Name Expires*, GO DADDY SUPPORT (May 21, 2012), http://support.godaddy.com/help/article/1289/what-happens-if-my-protected-domain-name-expires.
[58] Alyson Shontell, *The 25 Most Expensive Domain Names of All Time*, BUS. INSIDER (Dec. 23, 2012, 8:03 AM) http://www.businessinsider.com/the-20-most-expensive-domain-names-2012-12?op=1.

[59] Lamm, *supra* note 29, at 7-17.
[60] *Id.* at 8-9.
[61] Beyer & Cahn, *supra* note 24, at 42.
[62] Beyer & Cahn, *supra* note 17, at 151.
[63] Korzec & McKittrick, *supra* note 11, at 61.
[64] *Id.*
[65] Stored Communications Act, 18 U.S.C. § 1030(a)(2) & (c) (2008).
[66] Lamm, *supra* note 29, at 10-11.
[67] *Id.* at 10.
[68]Ajemian v. Yahoo!, 83 Mass.App.Ct. 565, 576-77 (2013) (holding that the probate court had jurisdiction over the dispute regardless of the provision found in the terms of service agreement).
[69] *See* Lamm, *supra* note 29, at 9-11.
[70] *See* Computer Fraud & Abuse Act,18 U.S.C. § 1030 (2008).
[71]Richard Downing, Deputy Section Chief, Dep't. of Justice, Statement before the House Judiciary Subcomm. on Crime, Terrorism and Homeland Security (Nov. 15, 2011) (available at http://www.justice.gov/criminal/pr/speeches/2011/crm-speech-1111151.html).
[72] *See,* Lamm, *supra* note 29, at 10-11.
[73] *See* Stored Communications Act, 18 U.S.C. § 2702 (2008).
[74] *See* Orin Kerr, *A User's Guide to the Stored Communications Act, and A Legislature's Guide to Amending It*, 72 Geo. Wash. L. Rev.1208, 1223 (2004).
[75] *Id*.
[76] Jury Verdict Form at 1-3, Cheng v. Romo, No. 11-cv-10007-DJC, 2013 WL 2245312 (D.Mass.).
[77] Cheng v. Romo, No11-10007-DJC, 2012 WL 6021369, at *1-3 (D.Mass. Nov. 28, 2012).
[78] *Id*.
[79] *See generally id.*
[80] Lamm, *supra* note 29, at 11.
[81] In re Facebook, No. C 12-80171 LHK (PSG), 2012 WL 7071331, at *1 (N.D. Cal. Sept. 20, 2012).
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *See* Perrone, *supra* note 33, at 190-92.
[88] Beyer & Cahn, *supra* note 17, at 142-46 (summarizing various state statutes addressing digital assets).
[89] *Id.*
[90] *Id.* at 143.
[91] *Id.* at 144.
[92] *Id.* at 144-46.
[93] *Id.* at 147.
[94]*Fiduciary Access to Digital Assets Act,* UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets (last visited June 9, 2013).
[95] *Draft Fiduciary Access to Digital Assets, supra* note 15, at 9-11.

[96] Beyer & Cahn, *supra* note 17, at 152.
[97] UNIF. PROBATE CODE § 3-709 (2010).
[98] *See* Korzec & Mckittrick, *supra* note 11, at 61.
[99] UNIF. PROBATE CODE § 3-709 (2010).
[100] *See id*.
[101] *See id*.
[102] *See* UNIF. PROBATE CODE § 3-703 (a) (2010).
[103] Beyer & Cahn, *supra* note 17, at 138-39.
[104] UNIF. PROBATE CODE § 3-709 (2010).
[105] UNIF. PROBATE CODE § 3-706 (2010).
[106] *See* I.R.C. § 2033 (2013).
[107] Beyer & Cahn, *supra* note 17, at 139.
[108] *PayPal User Agreement,* PAYPAL, https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=ua/UserAgreement_full&locale.x=en_US#7.%20Closing%20Your%20Account (last updated May 7, 2013).
[109] Beyer & Cahn, *supra* note 17, at 140.
[110] *See id*.
[111] *Id*.
[112] Lamm, *supra* note 29, at 33.
[113] *See id.* at 34.
[114] *Id.* at 33.
[115] *See id.*
[116] *See id.*
[117] *Id.* at 31.
[118] *WhoIs Behind That Domain?*, NETWORK SOLUTIONS, http://www.networksolutions.com/whois/index.jsp (last visited June 12, 2013).
[119] Lamm, *supra* note 29, at 41.
[120] *See id.* at 39.
[121] *See id.* at 38-39.
[122] *Id.* at 35.
[123] *Id.*
[124] Blachly & Walker, *supra* note 9, at 178-81 (describing various email service provider's policies in regards to fiduciary access).
[125] *See* Lamm, *supra* note 29, at 36.
[126] *Id.*
[127] *What Happens When a Deceased Person's Account is Memorialized,* Facebook Help Center, https://www.facebook.com/help/103897939701143/?q=what%20happens%20when%20you%20die&sid=0lZWBGb6FkQR2eTkz (last visited June 12, 2013).
[128] UNIF. PROBATE CODE § 3-709 (2010).
[129] *See iCloud Terms & Conditions,* APPLE LEGAL, http://www.apple.com/legal/internet-services/icloud/en/terms.html (last revised Sept. 13, 2012).
[130] *Options Available When a U.S. Yahoo! Account Owner Passes Away,* YAHOO! HELP, http://help.yahoo.com/kb/index?page=content&id=SLN9112&actp=search&viewlocale=en_US&searchid=1368405914648&locale=en_US&y=PROD_ACCT (last updated Jan. 14, 2013).

[131] Eric Slivka, *Apple Announces 40 Billion Store Downloads, Nearly 20 Billion in 2012,* MACRUMORS (Jan. 7, 2013) http://www.macrumors.com/2013/01/07/apple-announces-40-billion-app-store-downloads-nearly-20-billion-in-2012/.
[132]Horace Dediu, *iTunes Users Spending at the Rate of $40/yr,* ASYMCO (May 12, 2013, 4:51 PM) http://www.asymco.com/2013/05/12/user-spend-on-itunes/.
[133] *iCloud Terms & Conditions, supra* note 135.
[134] *See* Lamm, *supra* note 29, at 30.
[135] *See* Blachly & Walker, *supra* note 9, at 178-81.
[136] *Id.*
[137] *Id.*
[138]*Options Available When a U.S. Yahoo! Account Owner Passes Away, supra* note 136.
[139] *Can I Access the Dropbox Account of Someone Who Passed Away?,* DROPBOX, https://www.dropbox.com/help/488/en (last visited June 12, 2013).
[140] *iCloud Terms & Conditions*, *supra* note 135.
[141] Lamm, *supra* note 29, at 31.
[142] *See* Perrone, *supra* note 33, at 195-98.
[143] *See Id.*
[144] Beyer & Cahn, *supra* note 24, at 42-43.
[145] Korzec & McKittrick, *supra* note 11, at 62; *see also id.*
[146] *See generally Cheng*, 2012 WL 6021369.
[147] *See* Lamm, *supra* note 29, at 9-11.
[148] Korzec & McKittrick, *supra* note 11, at 62.
[149] *Id.*
[150] UNIF. PROBATE CODE § 3-709 (2010).
[151] Lamm, *supra* note 29, at 35.
[152] *Id.*
[153] *See* Lamm, *supra* note 29, at 33.
[154] *See id.* at 35.
[155] *Identities of Nearly 2.5 Million Deceased Americans Misused Each Year,* ID ANALYTICS (Apr. 23, 2012), http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php.
[156] *Identity Theft Growing, Costly to Victims,* USA TODAY (Apr. 14, 2013, 4:28 PM), http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/.
[157] *How to Detect Fraud & Identity Theft*, ALLY BANK, http://www.ally.com/security/how-to-detect-fraud-and-identity-theft.html (last visited June 6, 2013).
[158]Sid Kirchheimer, *Protecting the Dead From Identity Theft,* AARP BULL. (Mar. 6, 2013), http://www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html (advising how to protect a decedent's identity from theft).
[159]*IRTC Fact Sheet 117- Identity Theft and the Deceased: Prevention and Victim Tips,* IDENTITY THEFT RESOURCE CENTER (Jan. 24, 2013, 11:24 AM), http://www.idtheftcenter.org/artman2/publish/c_guide/Fact_Sheet_117_IDENTITY_THEFT_AND_THE_DECEASED_-_PREVENTION_AND_VICTIM_TIPS.shtml.
[160] *See id.*
[161] Lamm, *supra* note 29, at 47.
[162] *See id.* at 47- 48.