PIXAR FOR ESTATE PLANNERS: WHO GETS YOUR DIGITAL STUFF WHEN YOU'VE LOGGED OFF FOR THE FINAL TIME

A Presentation for the Iowa Trust Association Fall Conference
West Des Moines, Iowa
October 3, 2019

Robert K. Kirkland
Kirkland Woods & Martinsen LLP
132 Westwoods Drive
Liberty, MO 64068
Telephone: 816-792-8300
Facsimile: 816-792-3337
E-mail: bkirkland@kwm-law.com
Website: www.kwm-law.com

I. UNDERSTANDING THE DIGITAL PROPERTY ISSUE

A. As the number, complexity, types and value of digital property held by our clients increases, questions regarding the administration and disposition of such items are increasing as well.

1. According to a 2011 McAfee survey, the average value of a person's digital assets is $55,000!

2. The average individual has 25 passwords.

3. There are thirty million (30,000,000) Facebook accounts that belong to dead people!

4. Eighty-four percent (84%) of all U.S. adults use the internet at least occasionally (if the average income of the sample is at least $75,000, that number jumps to ninety-seven percent (97%)).

5. Seventy-six percent (76%) of all U.S. adults use a social networking site.

6. Consider how much this will change over the next five-ten years….

B. What is meant by the generic term, "digital property"?

1. The Uniform Fiduciary Access to Digital Assets Act ("UFADAA") defines a "digital asset" to mean "an electronic record in which an individual has a right or interest."

a. The term does not include an underlying asset or liability unless the asset or liability itself is an electronic record.

b. “Catalogue of electronic communications” is defined to mean information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person.

c. “Content of electronic communication” means information concerning the substance or meaning of an electronic communication which (A) has been sent or received by a user; (B) is in electronic storage by a custodian providing an electronic-communication service to the public or is carried or maintained by a custodian providing a remote-computing service to the public; and (C) is not readily accessible to the public.

2. Perhaps the term "digital property" is best understood by reviewing examples of the same.

a. Frequent flyer, hotel, credit card and other mileage awards and points (see www.colloquy.com).

(1) Airline rewards.

(A) United and American allow the transfer of these points upon death.

(B) Delta and Southwest do not allow a transfer upon death.

(2) Hotel points.

(A) Marriott, Starwood and Best Western allow transfer of points upon death.

(B) Hilton does not allow transfer of points upon death.

b. E-mail accounts.

c. Social networking accounts.

d. Voicemail accounts.

e. Online photographs and videos.

f. Photograph sharing accounts (i.e. Instagram).

g. Video sharing accounts (i.e. YouTube)

h. I-tunes and other electronically stored music.

i. Financial information accounts.

j. Web pages and blogs.

k. Online purchasing accounts (i.e. PayPal, Amazon).

l. Domain names.

m. Online sales accounts (i.e., eBay, Craigslist).

n. Intellectual property rights that are created and stored digitally.

o. Video games and related virtual assets.

(1) Bit coins, for example, are an exclusively online currency that are acquired by creation or are purchased through online exchanges.

(2) The overall value of all bit coins being traded is currently estimated to be above $1 billion in real dollars.

p. Residential or commercial real estate security system.

q. Any and all usernames and passwords and other security access to any of the foregoing.

r. Any other items or information stored on a desktop, laptop, tablet or other computer, peripheral drive, storage device, mobile telephone or any similar device.

s. All similar digital items which currently exist or may exist as technology develops in the future.

C. Why all the fuss? Why should we, as estate planners, care about digital property?

1. Particularly for our younger clients, there can be real value in such assets.

a. In 2010, a person sold several parcels of virtual real estate for $635,000.

b. In 2012, an investor purchased a large amount of virtual real estate for $2,500,000!

2. Although many items of digital property do not produce real financial value, our clients and their heirs attach tremendous sentimental value to many items of digital property.

3. One of the major risks with many items of digital property is security, particularly when the user becomes disabled or dies.

4. To prevent unwanted secrets from being discovered.

D. Helping the client identify his or her own digital property.

1. Ultimately, the estate planner's role is to strongly encourage your clients to develop and maintain a current list of digital property, as well as the security passwords and/or encryptions necessary to access such assets, as well as provide for the access and disposition of such property in their estate plans.

2. Although you cannot make them do it, urging your client to complete a digital asset inventory as part of the estate planning process, including usernames, passwords and special encryptions, will be vital to the ultimate fiduciary handling the client's property.

II. WHY IS DIGITAL PROPERTY UNIQUELY DIFFICULT TO DEAL WITH?

A. Federal and State Laws

1. Anti-Hacking Laws: "Hacking" generally means breaking into a computer system, frequently with the intention to alter or modify existing settings. Putting aside those who hack for fun but without the intent to harm (and whatever psychological and sociological issues may exist), there is a fundamental privacy issue, not to mention the obvious potential for harm - both in terms of damage

to one's technology and loss of data, and in terms of financial loss from the theft of personal information.

a. Every state has a statute prohibiting hacking and other types of unauthorized access to personal computer systems. See, e.g. RSMo. §§ 537.525, 569.095, 569.097, 569.099.

b. The Stored Communications Act ("SCA"), 18 U.S.C. Section 2701(a) et seq, part of the Electronic Communications Privacy Act (or "ECPA"), contains two relevant prohibitions for planners and internet service providers:

(1) 18 U.S.C. Section 2701(a), which concerns access to digital property, creates a criminal offense for anyone to "intentionally access…without authorization a facility through which an electronic communication service is provided", as well as to "intentionally exceed…an authorization to access that facility." This section does not apply to "conduct authorized…by a user of that service with respect to a communication of or intended for that user."

(2) 18 U.S.C. Section 2702, prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a

communication that is stored by or carried or maintained on that service; HOWEVER, disclosure is permitted "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service".

(3) In 2012, beauty queen Sahar Daftary fell 150 feet to her death in what was ruled a suicide. In an effort to overturn the suicide ruling, two family members obtained a subpoena to compel Facebook to turn over the decedent's Facebook account contents, believing the account contained evidence showing the decedent's actual state of mind in the days just prior to her death. The U.S. District Court in San Jose, California quashed the subpoena, holding that the Stored Communications Act, while permitting a provider (such as Facebook) to divulge the contents of a communication with the permission of the subscriber (here the decedent), does not require the provider to divulge the information. The court declined to address whether the family members could consent on the decedent's behalf.

(4) A later California Court of Appeal decision provided a 180 degree turn on the Stored Communications Act issue. The California Court held that, due to the fact that a Florida court had ordered a former employee of a company to give his express consent to disclosure of his e-mails in the process of discovery in a lawsuit filed against the employee by his former employer in Florida, whereupon the employee complied with that order by e-mailing Google and consenting to its production of e-mails sought. The California court held that this "express consent" takes the contemplated production of e-mails outside of the Stored Communications Act and permitted Google to make the requested disclosure. In doing so, the California Court of Appeals gave a different spin to the word "permissive" in the context of the consent exception to the Stored Communications Act prohibition against disclosure. Google argued that the Stored Communications Act allows but does not require disclosure by an electronic communication service provider if consent exists. The California Court of Appeals held that, insofar as the Stored

Communication Act permits a given disclosure, it permits a court to compel that disclosure under state law. Matteo Negro v. The Superior Court of Santa Clara, County, case number H040146, in the Court of Appeal of the State of California, Sixth Appellate District.

(5) In arguably the most important judicial decision since the digital property issues first came to the fore, the Supreme Judicial Court of Massachusetts held in Ajemian v. Yahoo! that a decedent's personal representative may provide lawful consent for the release of protected communications within the meaning of the SCA. The text of SCA § 2702(b)(3) does not specifically answer the question of whether the personal representative of a deceased individual may grant "lawful consent" on behalf of the deceased individual for the account provider to divulge the contents of protected communications. Prior court decisions have not answered this question. According to the Ajemian court, a decedent's personal representative can consent on the decedent's behalf to the release of the contents of the deceased user's email account.

(6) In Vista Marketing, LLC v. Burkett, 812 F.3d 954 (11th Cir. 2016), the 11th Circuit examined the case in which ex-wife allegedly violated the SCA when, following her lawyer's advice, she viewed her ex-husband's e-mails in an effort to prove to the divorce court that he was lying about and hiding assets. Although it was found that she was in technical violation of the SCA, the trial jury decided not to award the ex-husband any damages for this violation. The ex-husband appealed to the district judge, who declined to award him the claimed hundreds of thousands of dollars in damages and instead awarded him a very modest amount and no attorney's fees reimbursement. Ex-husband appealed to the 11th Circuit which held that, under the SCA, the court has no authority to award statutory damages in the absence of a showing of actual damages to the account holder.

(7) In Cheng v. Romo, 2013 U.S. Dist. LEXIS 179727 (Dec. 20, 2013), the United States District Court for the District of Massachusetts denied a motion for judgment notwithstanding a jury verdict affirming that Cheng was entitled to damages for Romo's

violation of the SCA and an invasion of privacy in violation of Massachusetts statutes. In this case, Romo admitted accessing a number of Cheng's e-mails that were stored in Cheng's Yahoo e-mail account by logging into Cheng's e-mail account using Cheng's password; however, Romo argued that at the time she read the e-mails, they had previously been opened by Cheng and, therefore, were not in "electronic storage" as that term is used in the SCA. The District Court was not impressed with Dr. Romo's creative argument.

(8) The SCA protects "contents" of a communication (i.e., the subject line and the body of a communication) and not non-content records (i.e., user's name and address, network IP address, and addressee's name and address). Also, the SCA does not apply to contents which are completely public.

c. The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. Section 1030, prohibits unauthorized access to computers.

(1) The U.S. Department of Justice takes the position that this Section supports a criminal charge when anyone "exceeds authorized access" by violating the access rules set forth in the provider's terms of

service agreement. There is NO specific exemption or authorization for fiduciaries attempting to access a decedent's digital assets.

(2) Virtually no one reads the terms of service agreement ("TOSA") when setting up online accounts. A recent university study centered around a fake website's TOSA, which included provisions indicating that the user's data would be shared with the NSA and that the user's first born child would be taken as payment for using this site. Notwithstanding these terms, 98% of the users agreed to the terms of the service agreement!

(3) There are a few cases which have addressed this issue directly.

(A) In United States v. Nosal, 676 F.3d 854 (9th Cir. 2012), the 9th Circuit held that written restrictions on the use of a computer, such as website terms of use or an employer's work place policy, do not control whether access is authorized. In this case, an employee of an executive search firm left that firm to set up a competitive shop, and he convinced his former co-workers to use their computer

system authorization to download information for him from the former employer's data base. The former employee was charged with aiding and abetting his former co-workers in exceeding their authorized access under the employer's terms of service agreement, and the 9th Circuit dismissed the indictment, holding that the phrase "exceeds authorized access" in the CFAA does not extend to violations of a company's "use restrictions" on the information obtained from the computer.

(B) The government later re-indicted Nosal, arguing that, after Nosal and his colleagues left their employer, they had no underlying legal right to access the company's computer network at all, and the use of a sympathetic current employee's log in credentials violated the "access without authorization" ban under the CFAA. This time, Nosal was convicted and the 9th Circuit upheld his conviction. The majority of the court held that since Nosal's former

employer had revoked his credentials, gaining the permission of a former co-worker to share a password constituted "access without authorization" under the CFAA. United States v. Nosal, Nos. 14-10037 & 14-10025 (9th Cir. July 5, 2016).

(C) A 2015 Second Circuit case involved a New York City cop who accessed the NYPD's computer system to search for a high school friend was in technical violation of the police department's computer use policy. He later used the information he obtained from the NYPD database in an online chat room, where he discussed kidnapping and cannibalizing his old friend (hence, he became known as the "Cannibal Cop"). However, he had not actually threatened anyone in those chats. He was charged with violating the CFAA but the trial judge acquitted him. The Second Circuit Court of Appeals upheld the acquittal, saying that the CFAA should be narrowly construed and should not support a conviction for a "mere"

TOSA violation. United States v. Valle, No. 14-2710-CR, 2015 WL 7774548 (2d Cir. Dec. 3, 2015)

(4) Some state's anti-hacking statements may be more strictly construed than the CFAA (i.e., Pennsylvania and Delaware).

d. Germany has not struggled with this issue like we have.

(1) In late April 2016, a Berlin regional court held that the parents of a deceased minor had the right to access their child's Facebook account.

(2) Applying common sense, the court reasoned that the digital messages were no different than written messages.

(3) Even though privacy is an important aspect of German law, the court held that a third-party sender had no more special right of privacy for online messages than they would for written messages.

(4) Facebook contested the matter vigorously, and an appeal is pending.

2. A few states, Connecticut, Delaware, Idaho, Indiana, Louisiana, Nevada, Oklahoma, Rhode Island, and Virginia all enacted very basic statutes regarding fiduciary access to a decedent's digital property prior to the Uniform Law Commission's endorsement of

"UFADAA" (the Uniform Fiduciary Access to Digital Assets Act). Although these states deserve some praise for initially tackling this issue, all but one of them fail to address the roadblocks created by federal law, as well as other factors.

a. Connecticut and Rhode Island gave the Personal Representative the power to access or copy the decedent's e-mail accounts.

b. Oklahoma and Idaho gave the Personal Representative the power to take control of, conduct, continue or terminate the decedent's e-mail, social networking, blogging or messaging service.

c. Nevada gave the Personal Representative the power to direct termination of any online account or similar electronic or digital asset of the decedent (but not to access or copy it!).

d. Indiana initially had the broadest statute, which allows the Personal Representative to access or copy the decedent's information stored electronically by a "custodian." It also attempts to require custodians to retain the decedent's electronic information for a two-year period after death.

e. Virginia passed a narrow statute that allows the Personal Representative of a deceased minor's estate to assume the obligations under a term of service agreement for purposes

of consenting to and obtaining disclosure of contents. Virginia initially has no statute with respect to an adult decedent's estate!

f. As discussed further below, Delaware enacted the Delaware Fiduciary Access to Digital Assets Act, which was effective as of January 1, 2015.

B. Service Provider Limitations

1. The home page of virtually every commercial website has a link at the bottom of the page to that website's Terms of Use. Signing up for an account on that website inevitably includes consenting to the site's Terms of Service Agreement ("TOSA"). From the standpoint of estate planning with regard to digital property, and later administration of a decedent's digital property, the Terms of Service are likely to be problematic.

a. The Yahoo! terms of service agreement provides: "You agree that your Yahoo! account is non-transferable 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."

b. Among Facebook's terms of service is the following: "You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do

anything else that might jeopardize the security of your account."

(1) Facebook allows a decedent's account to be "memorialized" - his or her profile remains available only to Facebook friends, and sensitive information is removed.

c. The Yahoo!, Facebook, and Google websites, among others, provide that their Terms of Service Agreements are governed by California law. If the account holder resides in Missouri and his or her digital property has its situs in Missouri, which state's law will apply in determining a fiduciary's access to a deceased account holder's digital property?

C. Technology Itself

1. Even if one has legal authorization to open someone else's electronic file or view the contents of a person's online account, access to the information will be impossible if the owner has protected the file or account with a strong password but has not provided access to the password.

D. Uncertainty as to web-based password management companies.

E. The hassle factor.

III. ESTATE PLANNING STRATEGIES FOR DIGITAL PROPERTY

A. A digital property inventory should be completed by the client.

1. See the attached Exhibit A for one form to give to your client for

this purpose (our Estate Planning Questionnaire has doubled in size as a result!).

2. This will take significant pushing and prodding by you, the planner, all within the time constraints of a fixed fee amount that your client is willing to pay.

3. The inventory should include an itemization of each item of digital property, along with all applicable passwords and encryptions.

B. Once the client has completed his or her inventory of digital property, what should he or she do with it?

1. A written list may be stored in one's safe deposit box, with a copy stored in the estate planner's file.

   a. Such a list may be outdated in a matter of months.

   b. Despite one's best intentions, a written inventory can be easily lost or destroyed.

2. A digitally stored inventory, secured by one password or encryption.

   a. This is more secure, less susceptible to loss or destruction, easier to maintain and update, and portable.

   b. There are free software and web-based services available for storage of passwords (i.e., Last Pass, Roboform, 1Password, Dashlane).

   c. Can the client be persuaded to go to this much "trouble"?

   d. One additional potential downside is, will the electronic

inventory also lock out the client's fiduciary?!

(1) There exist additional web-based services which assist fiduciaries and designated family members with access.

(2) For example, see www.deathswitch.com; others include Assets in Order, LegacyLocker, LegacyVault.

(3) For clients with extensive and potentially valuable digital property, they may want to combine the written inventory and electronically-stored list methods.

e. Passwords and encryptions can be a blessing and a curse:

(1) The security of your smart phones, computers, etc. is only as strong as the password used.

(2) Don't use a password that is easy to guess! Recently, a hacker stole the passwords of 32 million users from "RockYou, Inc.," a developer of games through social networking sites like Facebook. According to the New York Times, about 5,000 commonly used passwords would unlock 20% of these 32 million user accounts.

(3) Microsoft recommends passwords of at least 14 characters, using a mix of letters, numbers and

symbols.

(4) However, will you "lock out" your fiduciary in the process?! (Leonard Bernstein left his memoir on his death in electronic form with a password; to this day, no one has been able to access it, or help realize the financial value of it!)[1]

3. New Google service

a. In April, 2013, Google launched a new feature that facilitates a subscriber telling Google what he or she wants done with their Google account(s) when he or she dies or is no longer able to use such account(s).

b. The feature is called "Inactive Account Manager," which you can now find on your Google "Settings" page.

c. You can choose to have your digital data stored in the Google account deleted after a certain amount of inactivity, OR you can select trusted contacts to receive such data after the chosen period.

d. Before this system takes the chosen action, Google will first warn you by sending a text message to your mobile phone and an email to a secondary address you have provided.

4. New Facebook service

[1] Gunnarsson, Helen W., "Planning for Administering Your Digital Estate," 99 Ill.B.J.71 (2011).

a. Early in 2015, Facebook instituted a new "Legacy Contact" feature.

b. Go to www.facebook.com/help/1568013990080948, and you can designate someone to manage friend requests and other updates after death.

C. Making provision for access to the client's digital property upon the client's incapacity, with appropriate language in a durable power of attorney.

1. Sample clause: To access and obtain all digital or electronic data that may be stored on my desktop, laptop, tablet, or other computer, peripheral drive, storage device, mobile telephone or any similar device, including without limitation, all internet accounts (including e-mail accounts, iTunes, financial reports and archives of the same), on-line photographs and videos, on-line music, on-line documents, all licenses to on-line items and software, social network accounts, domain registrations, DNS service accounts, web hosting accounts, on-line stores, tax preparation service accounts, file sharing accounts, computer backup processes, and user passwords and other security access to any of the foregoing, and all similar digital items which currently exist or may exist as technology develops.

2. The planner should be sure to tailor the above clause for specific valuable digital property which a particular client has.

3. Even if your state statute includes such a power in its list of default or general powers for durable powers of attorney, RUFADAA requires that this power be specifically enumerated in your durable power of attorney form as to protected communications.

D. Similar provisions should be made in the decedent's estate planning documents for fiduciary access and handling of digital property during administration.

1. See Exhibit B for a sample Powers clause for your estate planning instruments.

2. The choice of fiduciary will also be key, if there is significant digital property.

3. In certain situations, consider using a "Special [Fiduciary]" specifically to handle digital property.

E. Provisions for ultimate disposition of digital property should be made in the decedent's estate planning documents.

1. In the decedent's will?

2. In the decedent's revocable trust?

F. Should the client be able to place a clause in his or her estate planning instrument providing for destruction of certain digital property (i.e., the "burn the Rembrandt" clause)?

1. Writings which the client has created.

2. "Private" e-mails and other digital correspondence.

G. Does the client want to leave digital property to anyone? (i.e., sensitive email exchanges, private financial transactions, etc.)

H. We also have our clients execute a standard Digital Asset Authorization, in the form attached hereto as Exhibit C.

I. Why is the planning stage so critical?

1. Identifying digital property with tremendous sentimental value.
2. Identifying digital property with real or potential fair market value.
3. Preservation and safekeeping of usernames, passwords and encryptions to protect security during the client's life and maintain such security upon the client's incapacity or death.
4. Immediate access to digital property upon the client's incapacity or death.
5. Providing the fiduciary immediate access to a treasure trove of the client's information immediately upon incapacity or death.
6. Empowering the client's fiduciary to protect such digital property during the pendency of estate administration.
7. Providing for an orderly transfer or termination of such digital property upon the client's demise.
8. Preserving evidence which is stored electronically, in case the client is involved in litigation at the time of his or her death or incapacity.
9. Indeed, the IRS is using electronically stored information to track

your clients and their assets. Among other things, IRS training manuals tell their agents to search the internet for a taxpayer's online activities, to review social media accounts in which the taxpayer participates, to search for domain names owned by the taxpayer, etc.

a. In its Chief Counsel Advice 201146017, the IRS advised that an IRS agent can summon a taxpayer's original electronic data files containing unaltered "metadata", as long as the information in the metadata "may be relevant" to a proper purpose for the IRS examination.

b. This is a critical ruling, as "metadata" contains a history of all document revisions, formulas and spreadsheets that are not printed, hidden text that is not printed and a record of who edited and reviewed the document as well as the dates and times of all revisions.

c. However, on April 16, 2013, the IRS Commissioner testified that their policy is not to seize "protected communications" without a search warrant.

J. Planning for the high net worth client.

1. Digital assets may be candidates for wealth transfer planning.

a. Intellectual property

b. Domain names

c. Bit coins or other cryptocurency

2. Consider utilizing digital property in wealth transfer planning.

a. Taxable gifts in trust

b. GRATs

c. Sales to IDGTs

IV. THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT ("UFADAA")

A. Background

1. In January, 2012, the Uniform Law Commission ("ULC") authorized the formation of a drafting committee to write model legislation that will give fiduciaries the authority to manage and control digital assets, copy or delete digital assets, and access digital assets.

2. It is important to realize that the scope of this drafting committee's assignment was to draft a model act that would govern access, and not ownership or the succession of ownership. The charge given the drafting committee did not include granting fiduciaries any greater rights to digital property than the original account holder enjoyed, and was not to set forth any methods for the distribution of digital assets. The UFADAA drafting committee consisted of several "Commissioners" from the ULC, American Bar Association "Advisors", and representatives of the National Academy of Elder Law Attorneys, the American Bankers Association, several companies which provide digital accounts, the

American College of Trust and Estate Counsel, the Uniform Law Conference of Canada, and other attorneys, judges and legislators from all over the country.

3. The UFADAA was developed initially in two separate two-day drafting meetings in December, 2012 and February, 2013, followed by a first reading at the ULC's July, 2013 annual meeting in Boston. The UFADAA was revised and revised again in two-day drafting meetings held in November, 2013 and March, 2014, prior to its final reading at the ULC's July, 2014 annual meeting in Seattle. By a vote of 50 to 0, the ULC approved UFADAA in its then "final" form which was followed by review and publication by the ULC Style Committee during September, 2014.

4. Despite a number of introductions/discussions of UFADAA as bills in multiple states, Delaware is the only state which adopted UFADAA. Indeed, the legislature in Delaware proceeded to adopt the final draft version of UFADAA prior to the ULC annual meeting in July, 2014, which was signed into law by the Governor of Delaware later in 2014.

5. The multiple 2015 bills were blocked by a coalition of internet providers and privacy advocates (i.e., the ACLU) who vehemently opposed the adoption of UFADAA in these approximately twenty-seven (27) states.

6. This led to renewed informal discussions between members of the UFADAA Enactment Committee, internet providers and privacy advocates. A revised model act was produced, which Facebook and other original opponents of UFADAA was acceptable. On July 15, 2015, the ULC approved a Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA"). It has now been enacted in forty-one (41) states and the U.S. Virgin Islands.

B. RUFADAA plays a critical role in the administration of digital assets, as it provides a clear roadmap for fiduciaries to follow to request access to digital account contents, which are otherwise "protected" under the SCA. Under RUFADAA, if the personal representative is rebuffed by an internet service provider, then he or she may apply for a state court order directing the provider to comply with his or her request.

C. The structure of RUFADAA

1. Section 1 sets forth the title of this Act.

2. Section 2 includes key definitions of terms used throughout the act.

a. Many of the definitions are based on those originally set forth in the Uniform Probate Code.

b. In other instances, the definitions attempt to mirror the definition of certain terms contained in federal law, including the Electronic Communications Privacy Act, and the Uniform Electronic Transactions Act.

c. The “terms-of-service agreement” definition originated in part from the definition of “agreement” found in Uniform Commercial Code Section 1-201(b)(3).

d. You should note the breadth of the definition of the word “digital asset”. The drafting committee went through at least half a dozen different definitions of this term before ending up with the current definition.

3. Section 3 sets forth the four types of fiduciary to which RUFADAA applies, and makes clear that the Act does not apply to any digital asset of an employer used by an employee. This Section now makes sure that this Act applies to a custodian (i.e., provider) of digital assets for a user IF the user resides in this state or resided in this state at the time of the user’s death.

4. RUFADAA Section 4 provides that users may consent to disclosure of their electronic communications, either online or in a record, and that such consent will override any TOSA provision to the contrary.

a. Without consent, providers are not required to disclose content.

b. If a user has not used an online tool to give direction as contemplated above, or if a custodian has not provided an online tool, a user may allow or prohibit disclosure to a

fiduciary of some or all of the user's digital assets, in a will, trust, power of attorney, or other record.

5. Section 5 makes clear that RUFADAA does not override a custodian's TOSA, except to give effect to the consent provisions of Section 4.

    a. Thus, if there is no advance planning by the user, then the TOSA will control fiduciary access.

6. Section 6 of RUFADAA sets forth the possible procedures for custodians to disclose the digital assets of a user under RUFADAA.

    a. The custodian may, in its sole discretion, grant the fiduciary full access to the user's account, or grant partial access to the user's account sufficient to perform the task with which the fiduciary is charged, or provide the fiduciary with a digital or paper copy of a digital asset

    b. If a custodian considers a user's direction or a fiduciary's request to impose an undue burden, either the custodian or the fiduciary may petition the court for an order clarifying the method of disclosure.

7. Section 7 of RUFADAA sets forth the rules for disclosure of protected electronic communications of a deceased user.

    a. If the user consented to disclosure of electronic communication contents, or if the court directs disclosure, a

custodian shall disclose to the personal representative of the estate of a deceased user the content of an electronic communication sent or received by the user, provided that the personal representative provides to the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) A certified copy of the death certificate of the user;

(3) A certified copy of the letters of appointment of the personal representative, or a small estate affidavit, or a court order;

(4) Unless the user provided direction using an online tool, then the personal representative shall provide a copy of the user's will, trust, power of attorney, or other record evidencing the user's consent to disclosure of the contents of electronic communication; and

(5) If requested by the custodian, the personal representative shall provide a number, user name or address assigned by the custodian to identify the user's account, evidence linking the account to the user, or an order of the court finding that (A) the user had a specific account with the custodian, identifiable by a number, user name or address

assigned by the custodian; (B) the disclosure of the content of the user's electronic communications will not violate federal privacy law; (C) unless the user provided direction using an online tool, the user consented to disclosure of the contents of electronic communications; or (D) disclosure of the contents of electronic communications of the user is reasonably necessary for estate administration.

8. RUFADAA Section 8 sets forth the disclosure requirements of non-protected digital assets of a deceased user.

   a. Unless the user prohibited disclosure of digital assets, or the court directs otherwise, a custodian shall disclose to the personal representative for the estate of a deceased user a catalog of electronic communications sent or received by the user.

   b. Additionally, unless the user prohibited disclosure or the court directs otherwise, a custodian shall disclose any other digital assets in which the user had a right or interest, except for protected contents of electronic communications.

   c. The personal representative must provide to the custodian (1) a written request for disclosure in physical or electronic form, (2) a certified copy of the death certificate of the user, (3) a certified copy of the letters of appointment of the

personal representative, or a small estate affidavit or a court order, and (4) if requested by the custodian, a number, user name or address assigned by the custodian to identify the user's account, evidence linking the account to the user, an affidavit stating that disclosure of the user's digital assets is reasonably necessary for estate administration, or an order of the court finding that (1) the user had a specific account with the custodian, identifiable by a number, user name or address assigned by the custodian, or (2) that disclosure of the user's digital assets is reasonably necessary for estate administration.

9. Section 9 of RUFADAA addresses the disclosure of contents of electronic communications of a principal to an agent under a power of attorney.

a. To the extent a power of attorney expressly grants an agent authority over the contents of electronic communications sent or received by the principal, and unless otherwise directed by the principal or the court, a custodian shall disclose to the agent the content of electronic communication sent or received by the principal, <u>if</u> the agent gives the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) An original or copy of the power of attorney expressly granting the agent authority over the contents of electronic communications of the principal to the agent;

(3) A certification by the agent, under penalty of perjury, that the power of attorney is in effect; and

(4) If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the principal's account; or (B) evidence linking the account to the principal.

10. Section 10 of RUFADAA addresses disclosure of non-protected digital assets to the agent under a power of attorney.

a. Unless otherwise ordered by the court, directed by the principal, or provided by a power of attorney, a custodian shall disclose to an agent with specific authority over digital assets or general authority to act on behalf of a principal a catalog of electronic communications sent or received by the principal, as well as any other digital assets in which the principal has a right or interest, except the protected contents of electronic communications.

b. The agent must provide to the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) An original or a copy of the power of attorney that gives the agent general authority to act on behalf of the principal;

(3) A certification by the agent, under penalty of perjury, that the power of attorney is in effect; and

(4) If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the principal's account; or (B) evidence linking the account to the principal.

11. Section 11 of RUFADAA addresses disclosure of digital assets held in trust when the trustee is the original user.

a. Unless otherwise ordered by the court or provided in the trust instrument, a custodian shall disclose to the trustee who is an original user, any digital asset held in trust, <u>including</u> any catalog of electronic communications of the trustee <u>and</u> the contents of an electronic communication.

12. Section 12 of RUFADAA deals with disclosure of protected electronic communications held in trust when the trustee is not the original user.

a. Unless otherwise ordered by the court, directed by the user, or provided in the trust instrument, a custodian shall disclose to a trustee who is not the original user the content of electronic communications sent or received by an

original or successor user and carried, maintained, processed, received or stored by a custodian in an account of the trust if the trustee gives to the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) A copy of the trust instrument or a certification of trust under the Uniform Trust Code, that includes consent to disclosure of the contents of electronic communications to the trustee;

(3) A certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust; and

(4) If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the trust's account; or (B) evidence linking the account to the trust.

13. Section 13 of RUFADAA addresses disclosure of non-protected digital assets held in trust when the trustee is not the original user.

a. Unless otherwise ordered by the court, directed by the user, or provided in the trust instrument, a custodian shall disclose to a trustee who is not an original user a catalog of electronic communications sent or received by an original or successor user and stored, carried, or maintained by a

custodian in an account of the trust, as well as any other digital assets in which the trust has a right or interest, other than protected contents of electronic communications.

b. The trustee must provide to the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) A certified copy of the trust instrument, or a certification of trust under the Uniform Trust Code;

(3) A certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust; and

(4) If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the trust's account; or (B) evidence linking the account to the trust.

14. Section 14 of RUFADAA addresses disclosure of digital assets to a conservator of a protectee.

a. The court having jurisdiction over the conservatorship, after an opportunity for a hearing under state law, may grant a conservator a right to access a protectee's digital assets.

b. Unless otherwise ordered by a court or directed by the user, a custodian shall disclose to that conservator a catalog of

electronic communications sent or received by the protectee, and any other digital assets in which the protectee has a right or interest, other than protected contents of electronic communications.

c. The conservator must provide to the custodian:

(1) A written request for disclosure in physical or electronic form;

(2) A certified copy of the court order that gives the conservator authority over the protectee's digital assets; and

a. If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the protectee's account, or (B) evidence linking the account to the protectee.

d. A conservator with general authority to manage the assets of a protectee may request a custodian of the protectee's digital assets to suspend or terminate an account of the protectee for good cause. A request made under this section shall be accompanied by a certified copy of the court order giving the conservator authority over the protectee's property.

15. In one of the more important sections of RUFADAA, Section 15 provides guidelines with respect to general fiduciary duty and authority as they relate to digital assets.

    a. The legal duties imposed on a fiduciary charged with managing tangible property also apply to the management of digital property, including the duties of care, loyalty, and confidentiality.

    b. Specifically, a fiduciary's authority with respect to a digital asset of a user is subject to the terms of service agreement, except as otherwise provided in Section 4 of RUFADAA; is subject to other applicable laws, including copyright law; is limited by the scope of the fiduciary duties; and may not be used to impersonate the user.

    c. A fiduciary with authority over the property of a decedent, protectee, principal or settlor, has the right to access any digital asset in which the decedent, protectee, principal or settlor had a right or interest and that is not held by a custodian or subject to a TOSA.

    d. A fiduciary acting within the scope of the fiduciary's duties is an authorized user of the property of the decedent, protectee, principal or settlor for the purpose of applicable computer-fraud and unauthorized-computer-access laws, including this state's laws.

e. A fiduciary with authority over the tangible personal property of a decedent, protectee, principal or settlor, has the right to access that property and any digital assets stored in it, and is an authorized user for purposes of any applicable computer-fraud and unauthorized-computer-access laws, including this state's laws.

f. A fiduciary may request termination of a user's account if termination will not violate any fiduciary duty. A request for account termination must be in writing, in either physical or electronic form, and accompanied by:

1. If the user is deceased, a certified copy of the death certificate of the user.
2. A certified copy of the letters of appointment of the representative or a small estate affidavit or court order, power of attorney or a trust instrument, giving the fiduciary authority over the account; and
3. If requested by the custodian, (A) a number, user name or address assigned by the custodian to identify the user's account, (B) other evidence linking the account to the user, or (C) an order of the court finding that the user had a specific account with the custodian, identifiable by a number, user name or address assigned by the custodian.

16. Section 16 provides for custodian compliance and custodian immunity

    a. Importantly, this section provides that a custodian, as well as its officers, employees and agents, are immune from liability for any act done in good faith in compliance with this model act.

17. Sections 17 through 21 contain several administrative provisions, including severability clause and effective date provisions. Interestingly, the Arkansas version of RUFADAA eliminated the severability clause, which would otherwise have preserved the effectiveness of other provisions of this Act despite the adjudicated invalidity of a particular provision of the Act.

V. ADMINISTERING THE DIGITAL ESTATE

A. Finding the Assets

1. The time-honored modus operandi of a fiduciary and her attorney searching through a decedent's/incapacitated person's papers in his workplace and at home, watching the decedent's mail for a 90-day cycle, and reviewing the decedent's tax returns and account statements, is simply sub-standard in this day and age.

2. If the client has planned ahead, the fiduciary's task will be made simpler. Regardless, the fiduciary will need to take several immediate steps, whether or not planning has occurred previously.

a. An immediate inventory of all possible digital property must be made.

b. It is critical to obtain physical and virtual access to the client's smart phone, iPad or other tablet, laptop computer, and all other digital equipment, and to keep them secure.

(1) As discussed above, the Revised Uniform Fiduciary Access to Digital Assets Act provides procedures for the fiduciary to "step into the shoes" of the principal/ward/settlor/decedent for purposes of access to digital property that is covered by state computer fraud and abuse acts (discussed above), and that may be released by providers under the SCA (i.e., not protected communications).

(2) Depending on the amount of digital property held by the decedent, consider the following additional steps out of an abundance of caution:

(A) Make a backup of the original data before beginning any search.

(B) Consider hiring a consultant who specializes in data recovery to assist the fiduciary in accessing the various devices.

(C) Beware of implications of state and federal privacy and computer hacking laws (discussed above).

(3) The fiduciary must act quickly; some online account providers will delete the data associated with a user account if such account isn't accessed for four-nine months, and will delete the user's account if it isn't accessed for eight-twelve months.

(4) What should a fiduciary do IF no planning has been done?

c. Timely notice to third party e-mail providers is critical for preserving information.

(1) What if the client maintained an e-mail account through an employer e-mail system?

(2) Many providers of free e-mail accounts will delete the decedent's account and its contents within a few months following notice of his or her death.

d. A quick inventory should be taken of online purchasing accounts (as well as all other financial information stored online).

e. Access or control of web pages, blogs, social networking accounts, home security systems, voicemail systems, etc. is

critical in order to prevent identity theft, as well as preserve and transfer sentimental information for the family.

f. Each terms of service agreement must be reviewed to ascertain (1) whether the account terminates at death; (2) whether the account is transferrable; (3) whether the agreement prohibits others from using the account; and (4) which state law governs the agreement.

g. Quickly determine the value, if any, of the decedent's digital property.

(1) This must be reported accurately on a probate inventory, probate and/or trust accountings, and accountings required of an agent operating under a durable power of attorney.

(2) If the client has a taxable estate for federal and/or state estate tax purposes, the applicable value must be reported accurately on the federal and/or state estate tax return.

(3) How is digital property valued?

(A) Comparables?

(B) Capitalization of an ascertainable revenue share?

(C) Historical cost?

(D) Attempts to sell the item on Ebay or similar marketplaces?

(E) Other traditional valuation methods?

(4) Examples of potentially valuable digital property:

(A) Intellectual property created by the client.

(1) Intellectual property is typically valued by looking at recent revenue streams, together with forecasted future revenue streams.

(2) Bear in mind that the person's death can impact the future value of the decedent's intellectual property.

(B) Advertising revenue stream from web pages and/or blogs.

(1) In November 2011, The Atlantic reported that the top ten blogs in America had an aggregate value of $785 million.

(C) Domain names.

(1) These domain names typically cost around $15 to $30 online.

(2) In 2012, the domain name "investing.com" sold for $2.45 million.

(3) In 2006, the domain name "diamond.com" sold for $7.5 million.

(4) In 2004, the domain name "beer.com" sold for $7 million.

(5) In 2010, the domain name "sex.com" sold for $14 million.

(6) Insurance.com sold for $35.6 million in 2010.

(7) Carinsurance.com sold for $49.7 million in 2010.

(D) Virtual currency (e.g. Bitcoins).

(E) Virtual real estate.

(F) Unused credit card or travel points.

(G) Refunds from online purchasing accounts (watch for credit balances).

(H) Contents of e-mails and social networking accounts of certain public figures may have value.

(I) What about downloaded music, books and other copyrighted material??

(1) Under the "first sale doctrine", as codified by Section 109 of the Copyright Act, the owner of a particular copy or phono record lawfully made is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of copy or phono record. 17 U.S.C. Section 109.

(2) In 2001 (a lifetime ago in the digital world), the United States Copyright Office rejected the extension of the first sale doctrine to the distribution of digital works in its report on the Digital Millennium Copyright Act.

(3) In a very limited technical decision, the Southern District Court of New York recently held that the first sale doctrine does not permit the sale of digital music files on or through a website that enabled users to buy and

sell "used" copies of songs. However, this decision is based on very unique facts and thus very limited in future application. Capitol Records, LLC v. ReDigi, Inc., Case No. 1:12-cv-00095-RJS (SDNY March 30, 2013). The court clarified that the first sale doctrine continues to protect a "lawful" owner's sale of her particular "phono record." The court further stated that the doctrine protects the sale of the device or hard drive containing the media. Therefore, it appears that the sale of a device containing legally acquired digital media files is protected by the first sale doctrine.

(4) Stay tuned on this issue (pun intended).

h. If there is a current or potential future law enforcement investigation or a civil lawsuit involving the deceased person, it is important to preserve potential electronic

evidence to avoid obstruction of justice or contempt charges.

(1) The fiduciary should not attempt to power on or access the smart phone, computer or other storage media until appropriate precautions have been made to preserve the original data and to preserve the chain of custody of the electronic evidence.

(2) Consider using an independent computer forensics company to make an exact image copy of the storage media in order to preserve the original data.

B. Unlocking the Data

1. Again, the fiduciary will have to deal with the problem of data that is protected in some manner. If the fiduciary does not have access to passwords and encryption keys that were used by the decedent, the data may simply be unavailable.

2. You may want to hire a consultant who specializes in data recovery or computer forensics to access the devices and data, especially if you have reason to believe there is significant value in the digital property.

EXHIBIT A

DIGITAL ESTATE INFORMATION

A. HARD COPY FILE LOCATIONS

Financial=

House Materials=

Personal records=

Historical record=

B. DEFAULT INFORMATION

User names=

Passwords=

Secret questions=

Mother's maiden name=

Grade school=

Street where grew up=

C. ELECTRONIC DEVICE ACCESS

Device	Website	Username	PIN	Password
Computer				
Windows				
Cell phone				
Tablet				
GPS				
DVR/TiVO				
Television				

D. INCOME TAXES

Item	Website	User Name	PIN	Password
Federal income tax payment				
State income tax payment				
Prior computerized tax returns				

E. BANKING

Institution	Website	User Name	Password	Other information
Checking				Icon=
Savings				Verbal password=

F. STOCK

Institution	Website	User Name	Password	Other Information

G. RETIREMENT

Institution	Website	User Name	Password	Other Information
				Account #= Security question answer= Balance as of _____: $

H. INSURANCE

Institution	Website	User Name	Password	Other Information
Health				
Life				

I. CREDIT CARDS

Institution	Website	User Name	Password	Other Information
American Express				
Visa				
Master Card				

J. DEBTS

Institution	Website	User Name	Password	Other Information
Mortgage				
Cars				
Student Loan				

K. BUSINESSES

Institution	Website	User Name	Password	Other Information
Amazon.com				
e-Bay.com				
Airlines				
Netflix				

L. UTILITIES

Institution	Website	User Name	Password	Other Information
Electric				
Gas				
Internet				
Phone (landline)				
Phone (cell)				

TV				
Trash				
Water				

M. SOCIAL MEDIA

Institution	Website	User Name	Password	Other Information
Facebook				
LinkedIn				
YouTube				

EXHIBIT B

DIGITAL PROPERTY PROVISION FOR A WILL

Powers and authorizations regarding digital property. The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information. I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to the personal representative: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law. The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private.

EXHIBIT C

DIGITAL ASSET AUTHORIZATION

Authorization and Consent for Release of Electronically Stored Information

I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my then-acting fiduciaries at any time: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. The terms used in this authorization are to be construed as broadly as possible, and the term "fiduciaries" includes an attorney-in-fact acting under a power of attorney document signed by me, a guardian or conservator appointed for me, a trustee of my revocable trust, and a personal representative (executor) of my estate.

This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law. This authorization is effective immediately. Unless this authorization is revoked by me in writing while I am competent, this authorization continues to be effective during any period that I am incapacitated and continues to be effective after my death.

Unless a person or entity has received actual notice that this authorization has been validly revoked by me, that person or entity receiving this authorization may act in reliance on the presumption that it is valid and unrevoked, and that person or entity is released and held harmless by me, my heirs, legal representatives, successors, and assigns from any loss suffered or liability incurred for acting according to this authorization. A person or entity may accept a copy or facsimile of this original authorization as though it were an original document.

Signed _____, 2015

_____
[NAME]

STATE OF MISSOURI)
) ss.
COUNTY OF _____)

On _____, 2015, before me, the undersigned, a Notary Public in and for the County and State aforesaid, personally appeared _____, to me known to be the person who executed the foregoing instrument, and acknowledged that he/she executed the same as his/her free act and deed.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my official seal on the day and year last above written.

_____
Notary Public

My appointment expires:

_____