Digital Assets and Cryptocurrency

or

What in the World is Bitcoin and Did My Client Own Any?

Northeast Florida Estate Planning Council
September 18, 2018

Eric Virgil, Esq.
The Virgil Law Firm
201 Alhambra Circle, Suite 705
Coral Gables, FL 33134
Telephone: (305) 448-6333
Email: eric@virgillaw.com
www.virgillaw.com

Protecting Digital Assets

I. What are Digital Assets?

"Digital assets" are electronic records in which an individual has a right or interest. They are transmitted or stored on digital devices such as smartphones and computers. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record. Digital assets can include items such as:

(a) Documents (MS Word, Adobe PDF, Excel spreadsheets, etc.);
(b) Internet sites such as domain names or blogs;
(c) Email accounts;
(d) Social media accounts (Facebook, LinkedIn, Instagram, etc.);
(e) Intellectual property rights;
(f) Gaming characters;
(g) Online user accounts (banks, PayPal, brokerage, utilities, creditors, etc.);
(h) Business information such as customer and inventory databases, client records, and internal business accounting information (this could be part of a regular firm's record keeping or an online enterprise as found on eBay);
(i) Cryptocurrency such as Bitcoin or Ethereum;
(j) Credits with online vendors such as iTunes; and
(k) Artistic content such as photographs.

For this outline, I will use definitions that were promulgated by the Digital Assets and Information Study Committee of the Real Property, Probate and Trust Law Section of The Florida Bar in their draft of the recently enacted Florida Fiduciary Access to Digital Assets Act (the "Digital Assets Act").[1] The Digital Assets Act establishes a new chapter of the Florida Statutes, Chapter 740.[2] The provisions of the Act are set forth in Sections 740.001 – 740.09. Section 740.002 contains definitions of terms.

Here are some definitions from the Digital Assets Act:

a. "Account" means an arrangement under a terms-of-service agreement in which the custodian carries, maintains, processes, receives, or stores a digital asset of the user or provides goods or services to the user.

[1] The Florida Fiduciary Access to Digital Assets Act was passed by the Florida Legislature and signed by the Governor in March 2016. The Act has an effective date of July 1, 2016.
[2] A copy of the Act is attached to this outline as Exhibit A.

b. "Content of an electronic communication" means information concerning the substance or meaning of the 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.

c. "Custodian" means a person that carries, maintains, processes, receives, or stores a digital asset of a user.

d. "Designated recipient" means a person chosen by a user through an online tool to administer digital assets of the user.

e. "Digital asset" means an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.

f. "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.

g. "Online tool" means an electronic service provided by a custodian which allows the user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or nondisclosure of digital assets to a third person. [3]

h. "Person" means an individual, estate, trust, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

i. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

[3] See, for example, Google's "Inactive Account Manager" tool. A copy of the description of this tool is attached to the materials as Exhibit B.

j. "Terms of service agreement" means an agreement that controls the relationship between a user and a custodian.[4]

k. "User" means a person that has an account with a custodian.

II. Where are Digital Assets Found?

Digital assets can be located on any digital device. For example, digital assets of a decedent may be located in one or more of the following places:

(a) Computers – home and office;
(b) Smartphones;
(c) Tablets;
(d) eReaders;
(e) Cameras;
(f) Memory cards and flash drives;
(g) CDs and DVDs;
(h) In the cloud (online).

III. How are Digital Assets Relevant to Probate Practitioners?

Digital assets have financial value and that value can be lost. According to a 2013 survey from McAfee, Americans valued their digital assets, on average, at between $35,000 to $55,000. This number is certain to be higher today. Eighty-five percent of Americans use the Internet and this is an area in which growth is rapid. The average person has 26 digital accounts and that number is higher as you deal with the younger population.

As of 2014, in just 60 seconds of Internet activity, there was an average of 25,000 items purchased through Amazon sales, 433,000 tweets, 5,000,000 videos viewed on YouTube, 293,000 statuses updated on Facebook, 15,000 songs downloaded from the Apple Store, and over 138,800,000 emails sent. A recent study found that 75% of families with an income in excess of $75,000 conduct banking online.

To the extent digital assets have financial value, they must be marshaled, declared on inventories, accountings, and on federal estate tax returns, and administered as part of the probate process. To the extent these items are neglected or lie dormant, they may be subject to risks such as losses due to hacking, copyright violations, and termination of service from account providers. To the extent digital accounts are set to automatically pay bills, the

[4] Terms of service agreements ("TOS") are those fine-print documents that pop up when establishing an online account. The computer dialog box containing the agreement typically requests that users check a box that says something like, "I have read all the terms and I agree," before the account can be created.

decedent's assets may be unnecessarily lost if these autopay arrangements are not reviewed by a personal representative.

Even those digital assets without financial value likely have a sentimental value to the decedent's survivors. These assets can include photographs, emails, Facebook pages, and other personal information.

Finally, even if digital assets do not have financial value or sentimental value they contain information that point to regular assets and liabilities that fiduciaries must administer.

IV. Problems Practitioners and Fiduciaries Face With Regard to Digital Assets

Until the passage of the Act, the biggest problem was lack of defined right of access for fiduciaries. The Florida Probate Code and Trust Code do not mention digital assets, does not define these assets, and do not contain clearly applicable rules governing access to them by fiduciaries. These issues have now been addressed by the Digital Assets Act.

More importantly, prior to the passage of the Digital Assets Act, access to digital assets created a minefield where fiduciaries could unknowingly violate both federal and state criminal law regarding hacking and privacy. Virtually none of these criminal laws have a provision for fiduciary access.

As a practical matter, even if they are willing to venture into this minefield, fiduciaries may be unable to find the decedent's login and password information or information may be encrypted.

Some issues attorneys are likely to encounter are the following:

1. Lack of planning. Even if the client had documents they may not contain digital assets provisions.
2. Lack of knowledge by clients, attorneys, and the court system regarding this topic. There will also be a lack of knowledge by tech companies regarding the application of the Digital Assets Act
3. Lack access/password issues, as noted above.
4. Indifference or hostility of tech industry to access even with the Digital Assets Act. The default position of the tech industry in the past was to deny access due to privacy concerns and their interpretation of federal law. The tech companies may also be confused by the interaction of existing TOS provisions with the Digital Assets Act.

V. What Law Applies to Digital Assets?

A. Florida Law

Florida law, beginning July 1, 2016, specifically addresses digital assets through the provisions of Chapter 740, Florida Statutes. This is the new Florida Fiduciary Access to Digital Assets Act. I will give a summary of the provisions of the Act and its operation later in the outline.

B. Federal Law

Federal law impacting access to digital assets relates to two areas: (1) privacy of digital information, and (2) unauthorized access to digital assets. Privacy is governed by the Stored Communications Act ("SCA") of 1986, 18 U.S.C. 2701-2711, as part of the Electronic Communications Privacy Act ("ECPA"). Unauthorized access issues are governed by the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030 (1986). Both these acts date from the pre-Internet late 1980s.

The SCA, in order to protect privacy rights of individuals, prohibits providers of public communications services from disclosing the content of user's communications to third parties except in situations similar to where a warrant is obtained. Under the SCA, the originator or the addressee/intended recipient of an electronic communication may provide lawful consent for disclosure. Unfortunately, fiduciaries are not mentioned in the legislation. One issue for fiduciaries is how to provide service providers with comfort that the fiduciary can give lawful consent to disclosure of SCA protected material. Among other things, contents of emails are communications likely protected by the SCA. Further, the concept of "lawful consent" only permits disclosure by an online service provider, it does not require disclosure. This issue was litigated recently in *In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things*, No. C 12 80171 LHK (N.D. Ca. Sept. 20, 2012). In that case, a decedent's family tried to compel Facebook to release account content. The court held that the SCA allowed only voluntary disclosure and that the service provider, Facebook, could not be compelled to disclose the account contents. The court did not rule on whether the personal representative possessed lawful consent of the decedent, but allowed Facebook to decide that issue.

The CFAA, on the other hand, governs access to the digital devices that would likely contain digital assets, such as computers. The CFAA requires authorization of the owner of the device in order to have lawful access. Unauthorized access is deemed to be illegal "hacking." Does a fiduciary have "authorization" of the owner to access a computer? If the fiduciary has been given express authorization, then clearly yes. If not, the law is unclear. Further, the law can be violated even with owner authorization if the fiduciary does not

have the service provider's authorization. Many providers' TOS prohibit third parties from accessing online accounts. When the fiduciary uses the account holder's authorization and login information to access an online account, does the fiduciary violate the law? Perhaps, if the access violates the TOS terms.

As a practical matter, federal and state criminal laws to prevent hacking and to preserve data privacy currently hinder disclosure and management of digital assets and information. See *Ajemian v. Yahoo!, Inc.*, 84 N.E. 3d 766 (Mass. 2017)(where there have been more than 8 years of litigation regarding the rights of the decedent's estate with regard to a Yahoo email account due to conflict regarding Yahoo's terms of service and the application of the SCA).

C. Contract Law Issues – TOS Problems

Service provider TOS frequently create legal issues related to access to digital assets. Some prohibit transfer of the assets under "indescendibility" provisions (Twitter, for example). The indescendibility concept arises from a provision in the TOS that the account/usage privileges merely constitute a license given to the account holder. Others may prohibit or inhibit fiduciary access (Instagram, Facebook, Yahoo, etc.).

D. The Solution – Florida Fiduciary Access to Digital Assets Act

The Digital Assets Act is a new stand-alone chapter of the Florida Statutes rather than legislation that addresses digital assets in piecemeal fashion in the Probate Code, the Trust Code, and so forth.[5] Here are some key provisions of the Act:

(a) F.S. Sec. 740.02 contains definitions of terms. Digital assets are defined broadly;

(b) F.S. Sec. 740.003 authorizes a user to use an online tool to allow a custodian to disclose or to prohibit a custodian from disclosing digital assets under certain circumstances;

(c) F.S. Sec. 740.004 provides for treatment of terms-of-service agreements;

(d) F.S. Sec. 740.005 provides procedures for the disclosure of digital assets generally;

(e) F.S. Sections 740.006 – 740.04 establish the rights of personal representatives, agents acting pursuant to a power of attorney, trustees, and guardians;

[5] A copy of the RPPTL Section's White Paper to the Florida Legislature, which sets forth the operation of the Act in detail and applicable law generally relating to digital assets, is attached as Exhibit C.

(f) F.S. Section 740.05 imposes fiduciary duties and provides for the responsibilities of a person acting in a fiduciary capacity;
(g) F.S. Section 704.06 requires compliance of a custodian and provides for immunity from liability for a custodian and its officers, employees, and agents acting in good faith in compliance;
(h) F.S. Sections 740.07 – 09 collectively, address miscellaneous issues, including making the effective date of the act July 1, 2016.

The Digital Assets Act is a solution to the bigger roadblocks to fiduciary access. The provisions of the Act will hopefully accomplish the following:

(a) Define digital assets and related terms;
(b) Provide clear default rules for fiduciary access under a variety of conditions;
(c) Allow for owner intent and privacy desires to control as the account user/owner's stated intent would govern whether the content of their electronic communications could be disclosed. The default rule for content of electronic communications would be non-disclosure unless the user indicates otherwise through an online tool (if utilized) or their estate planning documents.
(d) Encourages provider/custodian compliance and establishes clear procedures for provider/custodian interaction with fiduciaries;
(e) Provides protection from liability for fiduciaries and providers/custodians; and
(f) Clarifies that the Act is inapplicable to digital assets of employers used by employees in the ordinary course of the employer's business.

The Digital Assets Act takes a three-tiered approach generally to fiduciary access to digital assets. The three tiered approach is as follows:

1. A user's direction using an online tool prevails over an offline direction and over the terms-of-service if the direction can be modified or deleted at all times by the user.
2. A user's direction in a will, trust, power of attorney, or other record prevails over the boilerplate terms-of-service.
3. If a user provides no direction, the terms-of-service control, or other law controls if the terms-of-service are silent on fiduciary access.

The Act only governs access to digital assets. The underlying ownership and title of assets is not changed by the Act. Asset title and ownership would be governed by existing law. The Act was carefully written to fit into the framework

of the SCA and the CFAA so as not to be preempted by those laws but rather to fit into their scope in a defined way so that authorized access is clarified for all interested parties.

Finally, the legislation was part of a lengthy negotiation between tech industry representatives and the National Conference of Commissions on Uniform State Laws. This negotiation ultimately resulted in the Revised Uniform Fiduciary Access to Digital Assets Act of 2015 that was promulgated by the National Conference of Commissions on Uniform State Laws. The Revised Uniform Act was then tailored to Florida law in order to create the Digital Assets Act.[6]

VI. What Can be Done to Plan for and Protect Digital Assets?

A. Estate Planning - Advise Clients to Plan Ahead and Provide Tools

While estate planners, fiduciaries, and fiduciary counsel have perfected techniques used to transfer long-established types of property, most attorneys and fiduciaries have not yet determined how to address the disposition of digital assets. In addition, few owners of digital assets consider the fate of their online accounts or information once they are no longer able to manage these assets.

Consider asking your clients the following questions:

1. Who should have access to and control your online accounts/digital assets upon disability or death?
2. How will your fiduciaries discover all of your digital assets when needed?
3. How will your fiduciaries get access to these assets when that time comes?
4. In what way, if at all, do you want your digital assets to get transferred to your beneficiaries?
5. How should your digital assets be protected and preserved (or deleted if that is what the client desires)?
6. Do you own cryptocurrency, such as Bitcoin, and where are the public and private keys to that currency stored?

During the estate planning process, clients can be advised to plan ahead. Such planning includes advice to clients to do the following: (1) conduct a digital inventory; (2) back up (especially locally and to tangible media devices such as

[6] A detailed comparison of the original Uniform Fiduciary Access to Digital Assets Act, the Revised Uniform Fiduciary Access to Digital Assets Act, and a tech-industry promoted legislative effort known as the Privacy Expectations and Afterlife Choices Act (PEAC Act) is attached to the materials in the form of a table attached as Exhibit D to these materials. The Digital Assets Act operates like the Revised UFADAA in the table.

USB hard drives, flash drives, DVDs, etc.) their electronic information; (3) take advantage of any so-called online tool provided by an internet service provider of the client; and (4) make an estate plan that includes digital asset provisions. A tool for conducting a digital inventory is the My Digital Audit form attached to this outline as Exhibit E.[7]

The client should be informed they may supplement a paper record, such as My Digital Audit, with additional online measures. Online measures include: (1) use of an electronic service that safeguards passwords and logins, such as 1Password or LastPass; and (2) post-mortem online planning through companies like DeathSwitch, LegacyLocker, SecureSafe, that allow you to designate and approve access by fiduciaries prior to their appointment.

Additional steps you can advise clients to take:

1. Investigate whether accounts allow you to include designated agent in account preferences, such as "Facebook's "Legacy Contacts" and Google's "Inactive Account Manager." This is the so-called Online Tool defined in the Digital Assets Act.
2. Include explicit written permission in estate documents granting authorization to fiduciaries to access and control digital assets (see below).

In all of this planning, there is a security risk tradeoff the client must weigh in terms of giving vendors (or a third party such as the attorney) password information versus keeping passwords to themselves in a secure place such as a safe deposit box or some other secure location. There is significant hassle-cost with regard to this recordkeeping since password and login information changes regularly. I would not advise the attorney to keep this information for the client due to the security issues involved.

With regard to backed-up information, to the extent it is local this is helpful as it allows fiduciaries to avoid the current potential legal problems associated with accessing data stored remotely with service providers.

The client's estate planning documents should be drafted to include language aimed at administration of digital assets and information. Digital assets should be defined in the document if specifically devised. Fiduciary powers over digital assets should be set forth in the documents. One area that is evolving here is the possible use of trusts for digital assets that are otherwise "indescendible" (such as license-based assets that expire on death). Wills, of course, should not

[7] The author thanks James D. Lamm, Esq. of Minneapolis, MN, who graciously shared this form and shared additional information with the author in the preparation of this presentation. Mr. Lamm's blog, www.digitalpassing.com, is a great digital estate planning resource.

contain passwords or any login information since wills become public records during probate administration.

As noted above, one problem with planning ahead and doing digital audits is that logins and passwords frequently change; computers crash or wear out and are replaced. There is certainly a hassle-cost to this kind of planning but some planning is better than no planning.

One final tip relates to the email account-centric nature of digital assets. Most digital assets are linked to a particular email account of the account user/owner. Therefore, one (not several) personal (not work) email account should be linked to a person's digital assets. If a work email account is used, the fiduciary may not be able to access that account since an employer can lawfully deny access to the account.

B. Sample Forms (Use With Caution)

Sample forms[8] relating to fiduciary powers are set forth in Exhibits F (for powers of attorney), G (for wills), and H (for trusts).

Here is where the cautionary note, "with great power comes great responsibility," comes into play. You must understand that granting a fiduciary power to access digital assets means that fiduciary will have access to all your emails and will generally be able to see how you have used the Internet. Unless you specifically limit the fiduciary's access to digital assets, if you grant access in your estate plan then the fiduciary will see this information. This may lead to some uncomfortable conversations between couples who use the same lawyer for joint estate planning.

Given the comments above, please use caution with regard to any review of my suggested forms, as noted in the beginning of the outline. The forms are drafted broadly so to the extent a client desires to limit access that limitation needs to be drafted into the planning.

[8] The materials in this outline, and the attached exhibits and forms, are intended for continuing legal educational purposes only. They are not to be construed or relied upon as legal advice. The forms are sample forms only and should be used or adopted, if at all, only after careful independent consideration and review.

VII. How to Handle Probate of Digital Assets As the Law Evolves?

A. Select Appropriate Personal Representatives and Empower Them

The designated personal representative does not need to be a technical genius but should be able to work with or find people knowledgeable about computers and technology. If the personal representative is uncomfortable or unable to handle technical matters, consider recommending the retention of a computing expert to consult with the personal representative. The consultant can review digital issues, make recommendations for action to the personal representative, and leave the personal representative free to handle more traditional administration matters.

With regard to digital assets the personal representative should be granted the broad powers, including the power to hire consultants to assist the personal representative with appropriate actions. See Exhibit G for a sample powers clause for a will.

B. Steps the Personal Representative Can Take

Digital assets present new challenges for fiduciaries. Fiduciaries have duties with regard to these assets but no clear rights regarding access. With regard to determining assets and creditors, previously fiduciaries could rely on searches of paper records in homes, offices, and of items sent in the mail. Mail is now almost a thing of the past and people receive their notices, pay bills, conduct banking, and receive financial statements online. The personal representative also will be challenged in determining how to value digital assets. Finally, the personal representative will have to overcome electronic tripwires such as passwords and encryption.

Unless the decedent's will gives the personal representative specific authority to access digital assets, the personal representative should seek a specific court order for detailed authority to access digital assets and to hire consultants as necessary to assist in that regard.

The personal representative must determine which digital devices exist and their ownership. The devices used by the decedent and found by the personal representative (such as tablets or smartphones) may be owned by an employer or another person, so care needs to be taken to confirm ownership and the extent of the personal representative's authority over any devices.

Before the personal representative attempts to use the devices or power them on, the personal representative should consider retaining a computer consultant or forensics company to be the first to handle the devices. The

consultant can be directed to make exact copies of what is contained on the devices prior to any other action taking place. If the personal representative wants to attempt this individually, there is software available to assist with this task.

The retention of a computer expert can save the personal representative much time in determining what issues exist. Once the personal representative has access to the digital information of the decedent then the personal representative must determine what digital assets exist.

C. Determining What Digital Assets Exist in the Estate

Information located on smartphones, computers and email, and voicemail help you find digital assets located in online accounts/in the cloud. You should physically secure devices as they contain digital information but are also tangible personal property of the decedent (or of others).

Look for information about digital assets by searching the decedent's computer "favorites" folders and "favorites" websites, bookmarked websites, browsing history, and emails from accounts and service providers. Look for financial software or digital wallet software (for cryptocurrency such as Bitcoin) on devices. Video game characters and items, such as game property and points, can have financial value. Review income tax returns. Order a credit report for the decedent. Finally, the decedent may have data stored online (in the cloud). A combination of paper review and digital review will be required to determine the decedent's assets.

With regard to the decedent's devices, the personal representative should be advised to get the data from the devices and back that data up. Get help from a computer expert for how to get information off devices and access it in the first place if family members can't provide access and you don't have password information of the decedent.

D. Cryptocurrency – What is it and How to Find It?[9]

Cryptocurrency is digital currency. It was designed to work as a medium of exchange. It is nothing more than data sent from one user to another with cryptography used to make the transaction anonymous. Due to that cryptography, it can then be transmitted without being read by unauthorized persons.

[9] Substantial reference in the cryptocurrency sections of this outline was made to *Tales from the Crypt: What You Should Know (and Ask) About Cryptocurrencies* by Matt Triggs of Proskauer in Boca Raton, Florida, with his permission. Thanks to Matt.

The underlying technology that powers cryptocurrencies is known as "blockchain." Blockchain is a digital ledger that logs transactions in real time without the need for a single, centralized authority. Blockchain technology enables a group of users to record transactions in a ledger shared publicly by those users such that no transactions can be changed once published.

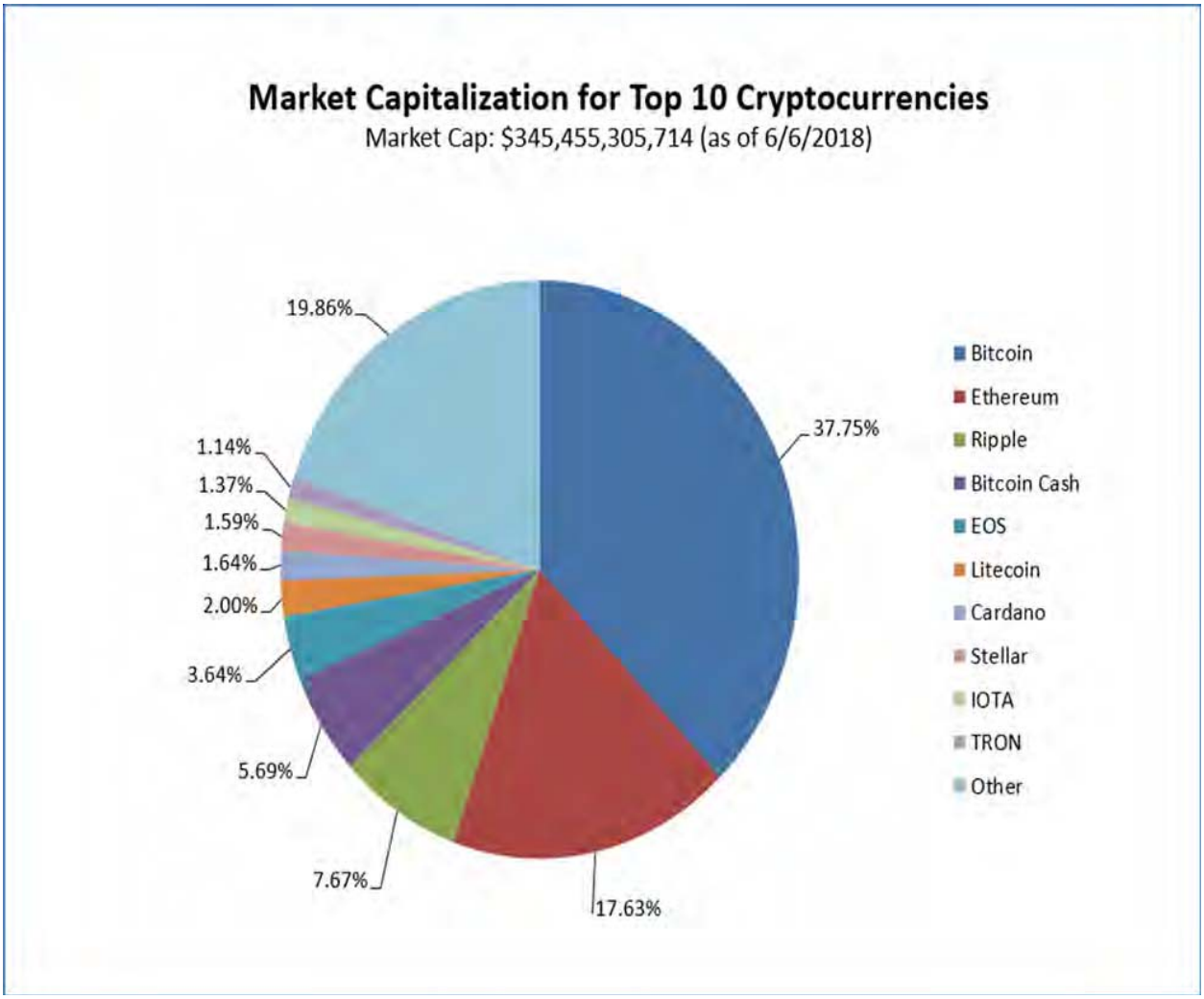
Whether cryptocurrency is actually "money" or not is subject to debate but it certainly can have monetary value and can be used to purchase some goods and services. There are now more than 1,000 cryptocurrencies with a combined market capitalization of over $400 billion dollars. These currencies provide an electronic payment system that enables paperless transactions from one person to another. Because cryptocurrencies are digital and direct, they bypass banks or credit card companies. It is important to note they are privately created and they are not backed by a central monetary authority such as the U.S. Federal Reserve.

1. Bitcoin as an Illustration

One way to understand cryptocurrency is to review the characteristics of the most popular and widely used cryptocurrency - Bitcoin. Bitcoin is generally described as a "convertible" cryptocurrency, because it has an equivalent value in traditional currency. The Bitcoin system is completely decentralized, meaning there are no servers involved and no central authority controlling Bitcoin transactions. From that standpoint, the system is vastly different from historical payment systems or government-issued currency. There is no bank or recognized central authority overseeing the Bitcoin system.

Bitcoin balances are kept by use of both public and private "keys." The public key is analogous to a bank account number, and it serves as the address that is published to the world and that can send and receive Bitcoins. The private key is analogous to a bank or computer password, or a digital signature. It is meant to be kept private from third parties, because it is the means by which Bitcoin transactions are accomplished. The public record representing the Bitcoin blockchain is available for anyone with the correct software to see, although the identity of any two transacting participants is anonymous. But because all transactions are recorded in the blockchain, it is theoretically impossible for the same person to sell the same Bitcoin to multiple purchasers. A Bitcoin owner's public key serves as the address that is published to the world and identifies where Bitcoins are held. The "address" is nothing more than a pattern of approximately 30 letters and numbers. But to own Bitcoins, or to transfer Bitcoins, an owner needs a corresponding private key for that address. Bitcoin transactions cannot be reversed. With limited exceptions, once a transaction is recorded in the blockchain, it cannot be modified.

To give a sense of the popularity of Bitcoin versus other virtual currencies, the chart below shows the relative market capitalization of the top ten virtual currencies, along with a catch-all for all others.



Bitcoin offers certain advantages, such as privacy, independence from country-specific monetary policies and substantial cost reductions for transactions. However, these advantages are offset by the risks presented by Bitcoin's volatility and questions regarding its long-term viability. Regarding volatility, Bitcoin's price changes frequently and rapidly. Bitcoin started 2017 at $997.72 and rose to $1,126.76 on January 4 — a change of almost 13% in just three days. By January 6, it had plummeted 21.6% to $883. That was the first of five separate 20% drops that Bitcoin experienced in 2017, the most recent being a 25% drop that took place between November 8 and November 12, when it fell to around $6,000. As of January 1, 2018, it was trading at around $13,400. As of September 1, 2018 it was trading around $7,300. This volatility in value is orders of magnitude higher than regular government currencies.

Although trading Bitcoin has become increasingly easy over time, most of it does not circulate in the real economy. Using it to buy things in common transactions is difficult, not just because it's not yet a widely accepted form of currency, but also because of the significant volatility mentioned above. Bitcoin is really more of a highly-risky speculative investment as opposed to currency. Consumers may be reluctant to spend them, as the value could spike significantly following the transaction; conversely, vendors may be reluctant to accept them, should their value plummet substantially after the transaction.

Any discussion of Bitcoin, and its risks and long-term viability, would be incomplete without discussing the sudden demise of what was once the largest Bitcoin exchange – the so-called Mt. Gox exchange. Mt. Gox unexpectedly collapsed in 2014, resulting in huge losses for Bitcoin investors. The collapse of the largest Bitcoin exchange is one of the many reasons that large financial institutions have expressed skepticism about cryptocurrency as an investment and that corporate trustees are declining to hold cryptocurrency in trust portfolios. Finally, there is the ever-present risk of losing one's private key which means losing access to the Bitcoin assets and there's no way to recover a key once the key is lost.[10]

Regardless of the risks, clients will be drawn to cryptocurrency for a variety of reasons so attorneys must understand where to look for client holdings. Cryptocurrency information, such as public and private keys, must be stored somewhere. This is commonly referred to as a "wallet." In the case of Bitcoin, the "wallet" doesn't actually hold Bitcoin. The "wallet" stores the public and private keys which allow the owner to send and receive Bitcoin. Estate planning and probate attorneys need to be aware of the wallet options that exist so they can advise clients and so they can determine where to look for the digital assets information. These include: storage on printed paper, storage on a local computer or laptop, offline storage on a flash drive, and hosted digital wallets online in the cloud through services such as Coinbase.

2. Case Law Related to Cryptocurrency

Is cryptocurrency "money?" Court decisions are mixed on this issue. Some courts have concluded that cryptocurrency is money, at least for certain legal purposes. *See Sec. & Exch. Comm'n v. Shavers,* No. 4:13-CV-416, 2014 WL 12622292, at *7 (E.D. Tex. Aug. 26, 2014) (holding that Bitcoin "has a measure of value, can be used as a form of payment, and is used as a method of exchange. As such, the Bitcoin investments in this case can satisfy the 'investment in money' prong set out by the Supreme Court in *Howey*."); see also *United States v. Ulbricht*, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014)

[10] The risks in holding Bitcoin for investment purposes, and issues related to its long-term viability, were recently described in an article published September 11, 2018 in the Wall Street Journal, titled *Olaf Carlson-Wee Rode the Bitcoin Boom to Silicon Valley Riches. Can He Survive the Crash?*

(concluding that Bitcoin is money within the context of the federal anti-money laundering statute). Other courts have taken a different view. See *In re Hashfast Technologies LLC*, No. 14-30725DM (Bankr. N.D. Cal. Feb. 19, 2016) (holding that, in a fraudulent transfer context, Bitcoin are not money); see also *State of Florida v. Michell Abner Espinoza*, No. F14-2923 (Fla. 11th Cir. Ct. 2016) (granting defendant's motion to dismiss information and noting "[t]his Court is not an expert in economics, however, it is very clear, even to someone with limited knowledge in the area, that [b]itcoin has a long way to go before it is the equivalent of money.").

Is cryptocurrency "property" for IRS tax purposes? At least one Federal district court has held "yes." *See United States v. Coinbase, Inc.*, No. 17-CV-01431-JSC, 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017). This is also the IRS's position pursuant to IRS Notice 2014-21, discussed later in this outline.

Is cryptocurrency subject to forfeiture proceedings by the government? Yes. *See United States v. 50.44 Bitcoins*, No. CV ELH-15-3692, 2016 WL 3049166, at *1 (D. Md. May 31, 2016).

3. Estate Administration of Cryptocurrency

The first issue, of course, is determining whether such an asset is even held by an estate. There won't be any monthly statements showing the asset. The decedent will not have received monthly statements. The cryptocurrency system is premised on anonymity. So how do you go about determining if a decedent held cryptocurrency? Set forth below are some suggestions:

1. Review of bank statements. Some online cryptocurrency exchanges allow purchases linked to bank account statements. Thus, a personal representative should examine bank statements for references to these online exchanges.
2. Review of credit card statements. Here too, some online exchanges allow linkage to credit cards for purchases. Thus, they should be reviewed for the same purpose.
3. Many cryptocurrency holders are computer experts with very high-powered computing equipment at home. Thus, an examination of the type of computer(s) owned by the decedent could provide some clues to a fiduciary.
4. Online custodial apps. Several online platforms provide for Bitcoin ownership through their own online wallet service. One popular, but by no means the only, one is Coinbase. A Bitcoin owner who uses such a service will not have direct access to his/her private key. Instead, the user will have a username/password type of access to an online platform and, in many cases, may have an app on his/her phone that will

allow for purchases and sales. Thus, personal computers and smartphones should be examined for such applications.

If Bitcoins are actually found in the decedent's estate, converting them to cash is a relatively straightforward matter. Conversion requires simply using an online exchange. These are for-profit businesses that connect buyers and sellers of Bitcoin. Prices offered by exchanges vary, so a personal representative should do some comparison shopping.

Actual distribution of the Bitcoin to beneficiaries should not be complicated. The simplest way is for the beneficiary to set up an online account with an online exchange so the fiduciary can transfer the Bitcoin to the beneficiary via the exchange. This is not the only transfer method but is one that is relatively simple to accomplish.

E. Procedures to Access Digital Assets under the Act

The procedures for a personal representative to request access to digital assets are set forth in F.S Sections 740.006-07 and 740.05. Generally this involves a written request accompanied by letters of administration and a copy of applicable provisions of the decedent's will (or a court order authorizing access).[11] The custodian then has three options for disclosing digital assets to the personal representative:

1. Allow the fiduciary to access the user's account.
2. Allow the fiduciary to partially access the user's account if sufficient to perform the necessary tasks.
3. Provide the fiduciary with a "data dump" of all digital assets held in the account.

Disclosure is required within 60 days, or the fiduciary may request an order of compliance. The order must contain a finding that disclosure does not violate 18 U.S.C. § 2702.

Deleted assets need not be disclosed. A request for some, but not all, of a user's digital assets need not be fulfilled if segregation is unduly burdensome. Instead, either party may petition the court for further instructions.

If termination would not violate a fiduciary duty, the fiduciary may request account termination rather than disclosure of assets. A custodian may require specific identification of the account and evidence linking the account to the user.

[11] Access procedures for trustees, agents, and guardians are similar to that for personal representatives but the specifics for each fiduciary are set forth in their own sections of the Act.

With regard to accounts with more than one authorized user, a custodian need not disclose if aware of any lawful access to the account after receipt of the disclosure request.

Finally, a custodian may assess a reasonable administrative charge for the cost of disclosing a user's digital assets.

The personal representative or counsel should review the TOS for the accounts, email and otherwise. In most cases, ownership of the account is not transferred to the fiduciary or family member. Terms for email providers can be restrictive (such as Yahoo) or more relaxed (such as Gmail). An email account may be deleted or terminated if not accessed or updated within 4 to 6 months. Email accounts should not be closed prior to ensuring that the decedent's financial information sent periodically by email (such as account statements and bills) and a record of the contents of the account have been saved. Email addresses should be changed with regard to delivery of financial information and bills.

If you can determine which financial institutions the decedent used, you can request paper copies of statements and information.

Determine whether the decedent had accounts with online sales organizations such as eBay, Amazon, or Craigslist (look for PayPal or Western Union information in records). Online purchasing accounts can be found through credit card receipts and bank receipts. Look for iTunes or Amazon cards. Credit card receipts can also show rewards programs, such as AMEX Member Rewards. For each rewards program discovered, the personal representative should contact the administrator of the program (i.e., AMEX) and follow their procedures in order to transfer the rewards points to the appropriate beneficiaries. A copy of the AMEX policy for transfer of rewards points is attached as Exhibit H.

Unfortunately, access to information and rewards points can be lost if accounts such as email accounts or credit card accounts are closed. As noted above, the personal representative should not close the decedent's accounts until full information regarding the account and any potential benefits in the account have been marshaled.

Webpage, domain name ownership, and blog information can be found through emails and credit card statements which set forth charges from providers or show reminders in emails to renew the domain. Domain ownership can be searched using WHOIS services and online services such as domaintools.com. Ownership of domains can be transferred to beneficiaries but new owner needs to confirm transfer.

Social networks should be contacted regarding death of the decedent. Their policies vary regarding what can be done post-death with the accounts.

To the extent digital accounts are set to autopay bills, the decedent's assets may be unnecessarily lost if autopay arrangements are not reviewed by a personal representative. However, make sure that online accounts are maintained until the personal representative can determine the value associated with those accounts and retrieve relevant information from the accounts.

The personal representative should consider wiping out the memory of the devices, using forensic deletion standards and software, prior to transferring them to the ultimate beneficiary. However, if the device is an e-reader or music device (like an iPod) the personal representative may want to consult with the beneficiary with regard to keeping books or music on the device.

F. How to Value Digital Assets?

Smartphones and computers have some value as tangible personal property. However, they need to be marshaled and examined mainly due to the data they contain. The value of the data itself is discussed further below.

Email accounts likely have little financial value unless the person was a celebrity. For online purchase and sales accounts (PayPal, Amazon, iTunes) review emails and statements to find them and then contact the institution to get cash balances as necessary. Online sales accounts may have value as ongoing business (may need business valuation).

Web pages and blogs normally have no financial value unless the decedent had a wide online audience. Social networking is similar to web pages and blogs in terms of financial valuation.

Domain names normally don't have value but may if popular terms are involved. Beer.com sold for $7 Million Dollars, vodka.com sold for $3 Million Dollars. Domain name appraisal services do exist (for example, Afternic).

Digital intellectual property rights may have value and, if so, are valued according to their past and future revenue streams.

With regard to games there is a market for gaming characters, items and currency depending upon the game and the decedent's level of achievement.

These assets may have different classifications. For example, computers and smartphones are tangible personal property. Domain names are intangible property. The personal representative will need to classify property appropriately.

Cryptocurrency has a monetary value which can be determined online depending upon the type of currency involved. IRS Notice 2014-21 provides guidance regarding the tax treatment of cryptocurrency. In the Notice, the IRS concluded that cryptocurrency is to be treated as property for federal tax purposes.

Given that treatment by the IRS, the following principles apply:

1. A taxpayer who receives cryptocurrency as payment for goods or services must include the fair market value of the currency as of the date the cryptocurrency was received. A taxpayer who "mines" cryptocurrency is taxed at the fair market value of the cryptocurrency as of the date of receipt, as it would be includable in gross income.
2. The basis of cryptocurrency that a taxpayer receives as payment for goods or services is equal to the fair market value of the currency as of the date of receipt.
3. The fair market value of cryptocurrency should be determined by reference to an exchange, if the cryptocurrency is listed on the exchange and the exchange rate is established by market supply and demand.

For federal transfer tax purposes, IRC Sec. 2031 and Reg. 20-2031-1(b) apply like they would to traditional property. This means you look for valuation information such as comparable sales, cash flows, and auction value. As you might suspect, since this is a new financial frontier the use of an expert to appraise the property will be advisable if currency exchange information is not readily available.

G. Finally, What About Music, Photos, and Apps?

Smartphones, e-readers, and other devices such as iPods will contain digital media such as music, books, photos, and apps. Look for iTunes and Amazon accounts of the decedent. Many times an account will have a cash balance that can be liquidated. With regard to photos online, review whether the decedent had accounts with photo sharing websites such as Flickr.

Can a personal representative sell or transfer digital media files without violating copyright laws? At this point you are likely asking for trouble if you sell or transfer files separately from the device itself so that is not recommended. See *Capital Records v. ReDigi*, 2013 WL 1286134 (S.D.N.Y. 2013).

Exhibit A

CHAPTER 2016-46

Committee Substitute for
Committee Substitute for Senate Bill No. 494

An act relating to digital assets; providing a directive to the Division of Law Revision and Information; creating s. 740.001, F.S.; providing a short title; creating s. 740.002, F.S.; defining terms; creating s. 740.003, F.S.; authorizing a user to use an online tool to allow a custodian to disclose to a designated recipient or to prohibit a custodian from disclosing digital assets under certain circumstances; providing that a specified user's direction overrides a contrary provision in a terms-of-service agreement under certain circumstances; creating s. 740.004, F.S.; providing construction; authorizing the modification of a fiduciary's or designated recipient's access to digital assets under certain circumstances; creating s. 740.005, F.S.; providing procedures for the disclosure of digital assets; creating s. 740.006, F.S.; requiring a custodian to disclose the content of electronic communications of a deceased user under certain circumstances; creating s. 740.007, F.S.; requiring a custodian to disclose other digital assets of a deceased user under certain circumstances; creating s. 740.008, F.S.; requiring a custodian to disclose the content of electronic communications of a principal under certain circumstances; creating s. 740.009, F.S.; requiring a custodian to disclose other digital assets of a principal under certain circumstances; creating s. 740.01, F.S.; requiring a custodian to disclose to a trustee who is the original user the digital assets held in trust under certain circumstances; creating s. 740.02, F.S.; requiring a custodian to disclose to a trustee who is not the original user the content of electronic communications held in trust under certain circumstances; creating s. 740.03, F.S.; requiring a custodian to disclose to a trustee who is not the original user other digital assets under certain circumstances; creating s. 740.04, F.S.; authorizing the court to grant a guardian the right to access a ward's digital assets under certain circumstances; requiring a custodian to disclose to a guardian a specified catalog of electronic communications and specified digital assets of a ward under certain circumstances; creating s. 740.05, F.S.; imposing fiduciary duties; providing for the rights and responsibilities of certain fiduciaries; creating s. 740.06, F.S.; requiring compliance of a custodian; providing construction; providing for immunity from liability for a custodian and its officers, employees, and agents acting in good faith in complying with their duties; creating s. 740.07, F.S.; providing construction; creating s. 740.08, F.S.; providing applicability; creating s. 740.09, F.S.; providing severability; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. <u>The Division of Law Revision and Information is directed to create chapter 740, Florida Statutes, consisting of ss. 740.001-740.09, Florida Statutes, to be entitled "Fiduciary Access to Digital Assets."</u>

Section 2. Section 740.001, Florida Statutes, is created to read:

740.001 Short title.—This chapter may be cited as the "Florida Fiduciary Access to Digital Assets Act."

Section 3. Section 740.002, Florida Statutes, is created to read:

740.002 Definitions.—As used in this chapter, the term:

(1) "Account" means an arrangement under a terms-of-service agreement in which the custodian carries, maintains, processes, receives, or stores a digital asset of the user or provides goods or services to the user.

(2) "Agent" means a person that is granted authority to act for a principal under a durable or nondurable power of attorney, whether denominated an agent, an attorney in fact, or otherwise. The term includes an original agent, a co-agent, and a successor agent.

(3) "Carries" means to engage in the transmission of electronic communications.

(4) "Catalog of electronic communications" means 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.

(5) "Content of an electronic communication" means information concerning the substance or meaning of the 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.

(6) "Court" means a circuit court of this state.

(7) "Custodian" means a person that carries, maintains, processes, receives, or stores a digital asset of a user.

(8) "Designated recipient" means a person chosen by a user through an online tool to administer digital assets of the user.

(9) "Digital asset" means an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.

(10) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(11) "Electronic communication" has the same meaning as provided in 18 U.S.C. s. 2510(12).

(12) "Electronic communication service" means a custodian that provides to a user the ability to send or receive an electronic communication.

(13) "Fiduciary" means an original, additional, or successor personal representative, guardian, agent, or trustee.

(14) "Guardian" means a person who is appointed by the court as guardian of the property of a minor or an incapacitated individual. The term includes an original guardian, a co-guardian, and a successor guardian, as well as a person appointed by the court as an emergency temporary guardian of the property.

(15) "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.

(16) "Online tool" means an electronic service provided by a custodian which allows the user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or nondisclosure of digital assets to a third person.

(17) "Person" means an individual, estate, trust, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

(18) "Personal representative" means the fiduciary appointed by the court to administer the estate of a deceased individual pursuant to letters of administration or an order appointing a curator or administrator ad litem for the estate. The term includes an original personal representative, a copersonal representative, and a successor personal representative, as well as a person who is entitled to receive and collect a deceased individual's property pursuant to an order of summary administration issued pursuant to chapter 735.

(19) "Power of attorney" means a record that grants an agent authority to act in the place of a principal pursuant to chapter 709.

(20) "Principal" means an individual who grants authority to an agent in a power of attorney.

(21) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(22) "Remote computing service" means a custodian that provides to a user computer processing services or the storage of digital assets by means of an electronic communications system as defined in 18 U.S.C. s. 2510(14).

(23) "Terms-of-service agreement" means an agreement that controls the relationship between a user and a custodian.

(24) "Trustee" means a fiduciary that holds legal title to property under an agreement, declaration, or trust instrument that creates a beneficial interest in the settlor or other persons. The term includes an original trustee, a cotrustee, and a successor trustee.

(25) "User" means a person that has an account with a custodian.

(26) "Ward" means an individual for whom a guardian has been appointed.

(27) "Will" means an instrument admitted to probate, including a codicil, executed by an individual in the manner prescribed by the Florida Probate Code, which disposes of the individual's property on or after his or her death. The term includes an instrument that merely appoints a personal representative or revokes or revises another will.

Section 4. Section 740.003, Florida Statutes, is created to read:

740.003 User direction for disclosure of digital assets.—

(1) A user may use an online tool to direct the custodian to disclose to a designated recipient or not to disclose some or all of the user's digital assets, including the content of electronic communications. If the online tool allows the user to modify or delete a direction at all times, a direction regarding disclosure using an online tool overrides a contrary direction by the user in a will, trust, power of attorney, or other record.

(2) If a user has not used an online tool to give direction under subsection (1) or if the custodian has not provided an online tool, the user may allow or prohibit disclosure to a fiduciary of some or all of the user's digital assets, including the content of electronic communications sent or received by the user, in a will, trust, power of attorney, or other record.

(3) A user's direction under subsection (1) or subsection (2) overrides a contrary provision in a terms-of-service agreement that does not require the user to act affirmatively and distinctly from the user's assent to the terms of service.

Section 5. Section 740.004, Florida Statutes, is created to read:

740.004 Terms-of-service agreement preserved.—

(1) This chapter does not change or impair a right of a custodian or a user under a terms-of-service agreement to access and use the digital assets of the user.

(2) This chapter does not give a fiduciary or a designated recipient any new or expanded rights other than those held by the user for whom, or for

whose estate or trust, the fiduciary or designated recipient acts or represents.

(3) A fiduciary's or designated recipient's access to digital assets may be modified or eliminated by a user, by federal law, or by a terms-of-service agreement if the user has not provided direction under s. 740.003.

Section 6. Section 740.005, Florida Statutes, is created to read:

740.005 Procedure for disclosing digital assets.—

(1) When disclosing the digital assets of a user under this chapter, the custodian may, at its sole discretion:

(a) Grant a fiduciary or designated recipient full access to the user's account;

(b) Grant a fiduciary or designated recipient partial access to the user's account sufficient to perform the tasks with which the fiduciary or designated recipient is charged; or

(c) Provide a fiduciary or designated recipient a copy in a record of any digital asset that, on the date the custodian received the request for disclosure, the user could have accessed if the user were alive and had full capacity and access to the account.

(2) A custodian may assess a reasonable administrative charge for the cost of disclosing digital assets under this chapter.

(3) A custodian is not required to disclose under this chapter a digital asset deleted by a user.

(4) If a user directs or a fiduciary requests a custodian to disclose under this chapter some, but not all, of the user's digital assets to the fiduciary or a designated recipient, the custodian is not required to disclose the assets if segregation of the assets would impose an undue burden on the custodian. If the custodian believes the direction or request imposes an undue burden, the custodian or the fiduciary may seek an order from the court to disclose:

(a) A subset limited by date of the user's digital assets;

(b) All of the user's digital assets to the fiduciary or designated recipient, or to the court for review in chambers; or

(c) None of the user's digital assets.

Section 7. Section 740.006, Florida Statutes, is created to read:

740.006 Disclosure of content of electronic communications of deceased user.—If a deceased user consented to or a court directs the disclosure of the content of electronic communications of the user, the custodian shall disclose to the personal representative of the estate of the user the content of an

electronic communication sent or received by the user if the personal representative gives to the custodian:

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

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

(3) A certified copy of the letters of administration, the order authorizing a curator or administrator ad litem, the order of summary administration issued pursuant to chapter 735, or other court order;

(4) Unless the user provided direction using an online tool, a copy of the user's will, trust, power of attorney, or other record evidencing the user's consent to disclosure of the content of electronic communications; and

(5) If requested by the custodian:

(a) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

(b) Evidence linking the account to the user; or

(c) A finding by the court that:

1. The user had a specific account with the custodian, identifiable by information specified in paragraph (a);

2. Disclosure of the content of electronic communications of the user would not violate 18 U.S.C. s. 2701 et seq., 47 U.S.C. s. 222, or other applicable law;

3. Unless the user provided direction using an online tool, the user consented to disclosure of the content of electronic communications; or

4. Disclosure of the content of electronic communications of the user is reasonably necessary for the administration of the estate.

Section 8. Section 740.007, Florida Statutes, is created to read:

740.007 Disclosure of other digital assets of deceased user.—Unless a user prohibited disclosure of digital assets or the court directs otherwise, a custodian shall disclose to the personal representative of the estate of a deceased user a catalog of electronic communications sent or received by the user and digital assets of the user, except the content of electronic communications, if the personal representative gives to the custodian:

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

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

(3) A certified copy of the letters of administration, the order authorizing a curator or administrator ad litem, the order of summary administration issued pursuant to chapter 735, or other court order; and

(4) If requested by the custodian:

(a) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

(b) Evidence linking the account to the user;

(c) An affidavit stating that disclosure of the user's digital assets is reasonably necessary for the administration of the estate; or

(d) An order of the court finding that:

1. The user had a specific account with the custodian, identifiable by information specified in paragraph (a); or

2. Disclosure of the user's digital assets is reasonably necessary for the administration of the estate.

Section 9. Section 740.008, Florida Statutes, is created to read:

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

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

(2) An original or copy of the power of attorney expressly granting the agent authority over the content of electronic communications 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, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the principal's account; or

(b) Evidence linking the account to the principal.

Section 10. Section 740.009, Florida Statutes, is created to read:

740.009 Disclosure of other digital assets of principal.—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

the digital assets or with general authority to act on behalf of the principal a catalog of electronic communications sent or received by the principal, and digital assets of the principal, except the content of electronic communications, if the agent gives the custodian:

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

(2) An original or a copy of the power of attorney which gives the agent specific authority over digital assets or 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, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the principal's account; or

(b) Evidence linking the account to the principal.

Section 11. Section 740.01, Florida Statutes, is created to read:

740.01 Disclosure of digital assets held in trust when trustee is the original user.—Unless otherwise ordered by the court or provided in a trust, a custodian shall disclose to a trustee that is an original user of an account any digital asset of the account held in trust, including a catalog of electronic communications of the trustee and the content of electronic communications.

Section 12. Section 740.02, Florida Statutes, is created to read:

740.02 Disclosure of content of electronic communications held in trust when trustee is not the original user.—Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose to a trustee that is not an original user of an account the content of an electronic communication sent or received by an original or successor user and carried, maintained, processed, received, or stored by the custodian in the account of the trust if the trustee gives the custodian:

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

(2) A certified copy of the trust instrument, or a certification of trust under s. 736.1017, which includes consent to disclosure of the content 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, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account; or

(b) Evidence linking the account to the trust.

Section 13. Section 740.03, Florida Statutes, is created to read:

740.03 Disclosure of other digital assets held in trust when trustee is not the original user.—Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose to a trustee that is not an original user of an account, a catalog of electronic communications sent or received by an original or successor user and stored, carried, or maintained by the custodian in an account of the trust and any digital assets in which the trust has a right or interest, other than the content of electronic communications, if the trustee gives the custodian:

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

(2) A certified copy of the trust instrument, or a certification of trust under s. 736.1017;

(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, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account; or

(b) Evidence linking the account to the trust.

Section 14. Section 740.04, Florida Statutes, is created to read:

740.04 Disclosure of digital assets to guardian of ward.—

(1) After an opportunity for a hearing under chapter 744, the court may grant a guardian access to the digital assets of a ward.

(2) Unless otherwise ordered by the court or directed by the user, a custodian shall disclose to a guardian the catalog of electronic communications sent or received by the ward and any digital assets in which the ward has a right or interest, other than the content of electronic communications, if the guardian gives the custodian:

(a) A written request for disclosure which is in physical or electronic form;

(b) A certified copy of letters of plenary guardianship of the property or the court order that gives the guardian authority over the digital assets of the ward; and

(c) If requested by the custodian:

1. A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the ward's account; or

2. Evidence linking the account to the ward.

(3) A guardian with general authority to manage the property of a ward may request a custodian of the digital assets of the ward to suspend or terminate an account of the ward for good cause. A request made under this section must be accompanied by a certified copy of the court order giving the guardian authority over the ward's property.

Section 15. Section 740.05, Florida Statutes, is created to read:

740.05 Fiduciary duty and authority.—

(1) The legal duties imposed on a fiduciary charged with managing tangible property apply to the management of digital assets, including:

(a) The duty of care;

(b) The duty of loyalty; and

(c) The duty of confidentiality.

(2) A fiduciary's or designated recipient's authority with respect to a digital asset of a user:

(a) Except as otherwise provided in s. 740.003, is subject to the applicable terms-of-service agreement;

(b) Is subject to other applicable law, including copyright law;

(c) In the case of a fiduciary, is limited by the scope of the fiduciary's duties; and

(d) May not be used to impersonate the user.

(3) A fiduciary with authority over the tangible personal property of a decedent, ward, principal, or settlor has the right to access any digital asset in which the decedent, ward, principal, or settlor had or has a right or interest and that is not held by a custodian or subject to a terms-of-service agreement.

(4) A fiduciary acting within the scope of the fiduciary's duties is an authorized user of the property of the decedent, ward, principal, or settlor for the purpose of applicable computer fraud and unauthorized computer access laws, including under chapter 815.

(5) A fiduciary with authority over the tangible personal property of a decedent, ward, principal, or settlor:

(a) Has the right to access the property and any digital asset stored in it; and

(b) Is an authorized user for the purpose of computer fraud and unauthorized computer access laws, including under chapter 815.

(6) A custodian may disclose information in an account to a fiduciary of the user when the information is required to terminate an account used to access digital assets licensed to the user.

(7) A fiduciary of a user may request a custodian to terminate the user's account. A request for termination must be in writing, in paper or electronic form, and accompanied by:

(a) If the user is deceased, a certified copy of the death certificate of the user;

(b) A certified copy of the letters of administration; the order authorizing a curator or administrator ad litem; the order of summary administration issued pursuant to chapter 735; or the court order, power of attorney, or trust giving the fiduciary authority over the account; and

(c) If requested by the custodian:

1. A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

2. Evidence linking the account to the user; or

3. A finding by the court that the user had a specific account with the custodian, identifiable by the information specified in subparagraph 1.

Section 16. Section 740.06, Florida Statutes, is created to read:

740.06 Custodian compliance and immunity.—

(1) Not later than 60 days after receipt of the information required under ss. 740.006-740.04, a custodian shall comply with a request under this chapter from a fiduciary or designated recipient to disclose digital assets or terminate an account. If the custodian fails to comply, the fiduciary or designated recipient may apply to the court for an order directing compliance.

(2) An order under subsection (1) directing compliance must contain a finding that compliance is not in violation of 18 U.S.C. s. 2702.

(3) A custodian may notify a user that a request for disclosure or to terminate an account was made under this chapter.

(4) A custodian may deny a request under this chapter from a fiduciary or designated recipient for disclosure of digital assets or to terminate an

account if the custodian is aware of any lawful access to the account following the receipt of the fiduciary's request.

(5) This chapter does not limit a custodian's ability to obtain or require a fiduciary or designated recipient requesting disclosure or termination under this chapter to obtain a court order that:

(a) Specifies that an account belongs to the ward or principal;

(b) Specifies that there is sufficient consent from the ward or principal to support the requested disclosure; and

(c) Contains a finding required by a law other than this chapter.

(6) A custodian and its officers, employees, and agents are immune from liability for an act or omission done in good faith in compliance with this chapter.

Section 17. Section 740.07, Florida Statutes, is created to read:

740.07 Relation to Electronic Signatures in Global and National Commerce Act.—This chapter modifies, limits, and supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. ss. 7001 et seq., but does not modify, limit, or supersede s. 101(c) of that act, 15 U.S.C. s. 7001(c), or authorize electronic delivery of any of the notices described in s. 103(b) of that act, 15 U.S.C. s. 7003(b).

Section 18. Section 740.08, Florida Statutes, is created to read:

740.08 Applicability.—

(1) Subject to subsection (3), this chapter applies to:

(a) A fiduciary acting under a will, trust, or power of attorney executed before, on, or after July 1, 2016;

(b) A personal representative acting for a decedent who died before, on, or after July 1, 2016;

(c) A guardian appointed through a guardianship proceeding, whether pending in a court or commenced before, on, or after July 1, 2016; and

(d) A trustee acting under a trust created before, on, or after July 1, 2016.

(2) This chapter applies to a custodian if the user resides in this state or resided in this state at the time of the user's death.

(3) This chapter does not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business.

Section 19. Section 740.09, Florida Statutes, is created to read:

740.09 Severability.—If any provision of this chapter or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are severable.

Section 20. This act shall take effect July 1, 2016.

Approved by the Governor March 10, 2016.

Filed in Office Secretary of State March 10, 2016.

Exhibit B

Google | Public Policy Blog

Updates on technology policy issues

Plan your digital afterlife with Inactive Account Manager

Posted: Thursday, April 11, 2013

Posted by Andreas Tuerk, Product Manager

Not many of us like thinking about death — especially our own. But making plans for what happens after you're gone is really important for the people you leave behind. So today, we're launching a new feature that makes it easy to tell Google what you want done with your digital assets when you die or can no longer use your account.

The feature is called Inactive Account Manager — not a great name, we know — and you'll find it on your Google Account settings page. You can tell us what to do with your Gmail messages and data from several other Google services if your account becomes inactive for any reason.

For example, you can choose to have your data deleted — after three, six, nine or 12 months of inactivity. Or you can select trusted contacts to receive data from some or all of the following services: +1s; Blogger; Contacts and Circles; Drive; Gmail; Google+ Profiles, Pages and Streams; Picasa Web Albums; Google Voice and YouTube. Before our systems take any action, we'll first warn you by sending a text message to your cellphone and email to the secondary address you've provided.

We hope that this new feature will enable you to plan your digital afterlife — in a way that protects your privacy and security — and make life easier for your loved ones after you're gone.

Labels

Archive

Feed

Follow @googlepubpolicy

Give us feedback in our Product Forums.

Exhibit C

WHITE PAPER

PROPOSED ENACTMENT OF CHAPTER 740, FLORIDA STATUTES

I. SUMMARY

The proposed legislation is a result of a study by the Digital Assets Committee of The Real Property, Probate and Trust Law Section of The Florida Bar of the Revised Uniform Fiduciary Access to Digital Assets Act. The proposal would add a new Chapter to the Florida Statutes that follows the proposed uniform act.

Under present Florida law, there is no legislation on fiduciary access to digital assets, only criminal laws regarding access to stored communications. The purpose of this act is to vest fiduciaries with certain authority to access, control, or copy digital assets and accounts. The Florida Fiduciary Access to Digital Assets Act ("FFADAA") addresses four different types of fiduciaries: personal representatives of decedents' estates, guardians of the property of minors or incapacitated persons, agents acting pursuant to a power of attorney, and trustees.

II. CURRENT SITUATION

As the number of digital assets held by the average person increases, questions surrounding the disposition of these assets upon the individual's death or incapacity are becoming more common. These assets range from online gaming items to photos, to digital music, to client lists. And these assets have real value: according to a 2011 survey from McAfee, Intel's security-technology unit, American consumers valued their digital assets, on average, at almost $55,000.[1] Few holders of digital assets and accounts consider the fate of their online presences once they are no longer able to manage their assets. There are millions of Internet accounts that belong to decedents. Some Internet service providers have explicit policies on what will happen when an individual dies, others do not; even where these policies are included in the terms of service, most consumers click through these agreements. Few laws exist on the rights of fiduciaries over digital assets.

The **current federal legislation** that dictates access to digital assets is buried in the Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA"), both passed in 1986, with only minor revisions since. The CFAA and similar state laws impose criminal penalties and perhaps civil liability too for the unauthorized access of computer hardware, devices, and stored data. These laws are explained in more detail below.

[1] Kelly Greene, *Passing Down Digital Assets*, WALL STREET JOURNAL (Aug. 31, 2012), http://goo.gl/7KAaOm.

Under **current Florida law**, Florida has enacted statutory counterparts to the provisions of the SCA and located them in Chapter 934, entitled "Security of Communications"[2] and in Chapter 815, entitled "Florida Computer Crimes Act". There is no legislation on fiduciary access to digital assets.

A minority of **other states** has enacted legislation on fiduciary access to digital assets, including Delaware, Connecticut, Idaho, Indiana, Oklahoma, Rhode Island, Nevada, and Virginia, and the existing statutes grant varying degrees of access to different types of digital assets. In addition, numerous other states have considered, or are considering, legislation. Existing legislation differs with respect to the types of digital assets covered, the rights of the fiduciary, the category of fiduciary included, and whether the principal's death or incapacity is covered.

The **National Conference of Commissioners on Uniform State Laws** at its annual conference July 2015 passed the **Revised Uniform Fiduciary Access to Digital Assets Act (2015)** (the "Revised UFADAA"). The Act specifically addresses how a fiduciary addresses digital assets. The commissioners on the drafting committee received input from estate attorneys, educators, and lawyers with expertise in various areas of the law affected by digital assets, advisors from the American Bar Association, representatives from service providers, such as Facebook and Yahoo, policy counsel from NetChoice (a trade association of eCommerce businesses and on-line consumers), and General Counsel from the State Privacy and Security Coalition, Inc. (which is comprised of 20 communications, technology, and media companies).[3]

The Revised UFADAA took into account the **Supremacy Clause of the U.S. Constitution**. According to the Supremacy Clause, "This Constitution, and the laws of the United States which shall be made in pursuance thereof.... *shall be the supreme law of the land,* and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary, notwithstanding."[4] The Supreme Court has ruled that a federal law that conflicts with a state law "preempts" the state law and that state laws that conflict with federal law are "without effect."[5] Due to the Supremacy Clause and the Supreme Court's interpretation, one major challenge in drafting the uniform act was that it does not directly conflict with existing federal law and could survive a constitutional challenge.[6]

It is what the **SCA** *does not specifically address* that gave rise to the Revised UFADAA proposed state law that the Uniform State Laws Commissioners believed can be legally interpreted as filling in the gaps of the SCA, as opposed to conflicting with it. The SCA was originally written to provide Fourth Amendment-like[7] privacy protection

---

[2] *Tracey v. State, 69 So.3d 992* (Fla. 4th DCA 2011).

[3] "Surf the Evolving Web of Laws Affecting Digital Assets" Bissett, W. and Kauffman, D. 41 Estate Planning No. 4 April 2014.

[4] U.S. Const. Art. VI (Emphasis added.)

[5] Maryland v. Louisiana, 451 U.S, 725 (1981).

[6] "Surf the Evolving Web" at 34.

[7] The Fourth Amendment to the U.S. Constitution protects the "people's rights to be secure in their houses, *papers, and effects,* against unreasonable searches and seizures." (Emphasis added.)

for certain types of email communications, social networking accounts, and other digital assets stored on a remote server. "The SCA attempts to modernize the reasonable expectation of privacy provided by the Fourth Amendment and later the Supreme Court to include two types of online services, "electronic communication services" and "remote computing services". To provide this privacy protection, the SCA limits the ability of the government to *compel disclosure* of both "non-content" information (i.e., logs of email communications including addresses of recipient/senders (analogous to the envelope of a letter)) as well as the "content" (what is inside the letter). The SCA also limits the ability of those internet service providers ("ISPs") that are "subject to" the SCA to reveal "content" information to non-government entities."[8] In general, the SCA states that certain service providers are permitted to disclose "non-content" information of electronic communications and files to anyone except the government without the consent of the user. However, a service provider *may* divulge the "content" of an electronic communication to a non-government entity *only* when the user lawfully consents.[9]

Like the SCA, the **CFAA** similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." Neither the SCA nor the CFAA specifically provides for or denies a fiduciary access to electronic and stored communications. In essence, even if consent was granted to a fiduciary, current federal law does not acknowledge the potential for such a vested right.[10]

The Revised UFADAA uses well-established, existing law for non-digital probate assets in order to provide **a fiduciary the right to "step into the shoes"** of a decedent to manage digital assets. However, the Revised UFADAA draws a sharp distinction between disclosing a catalogue of "non-content" communications (the outside of the envelope information described earlier) as opposed to the underlying content (what is inside the letter). If certain conditions are met, a catalogue may be provided to a decedent's fiduciary without express prior consent, whereas the actual content may only be provided with express prior consent (and subject to numerous conditions). Because the fiduciary has the same authority as the deceased user (no more and no less), the fiduciary is "authorized" by the deceased user as required under the two federal statutes (the SCA and CFAA) that prohibit unauthorized access.

The Revised UFADAA was also drafted in light of the fact that deceased users likely registered with on-line services for email, on-line purchases, photo sharing, on-line banking, and a long list of other items now done on-line by first consenting to a terms-of service agreement ("TOSA"). The Revised UFADAA recognized that in most situations the user likely consented to the TOSA by clicking "I agree" without ever reading it. These TOSAs generally describe the user's rights in using the service, how personal information will be protected, the conditions on information sharing, and user's rights (if any) upon death. The Revised UFADAA introduces the concept of an "online tool" for directing fiduciary access. An online tool is defined as an electronic service provided by a

[8] "Surf the Evolving Web" at 34 (citations omitted).
[9] 18 U.S.C. section 2702(b)(3).
[10] "Surf the Evolving Web" at 34 (citations omitted).

custodian that is distinct and separate from the TOSA.[11] The Revised UFADAA expressly permits a custodian to offer an online tool and provides that a direction regarding disclosure using an online tool supersedes a contrary direction in a will, trust, or power of attorney and over the TOSA (provided the online tool is available at all times). In the absence of an online tool directive, the deceased user's direction in a will, trust, power of attorney, or other record prevails over the blanket TOSA, or if no written direction, the TOSA will control.

Because of issues like the federal Supremacy Clause, the interest of ISPs in differing jurisdictions, privacy concerns, and overriding TOSA, the Florida drafting committee closely adhered to the careful analysis and drafting set forth within the Revised UFADAA, deviating from the proposed uniform law minimally, only where necessary to comport with Florida law.

III. EFFECT OF PROPOSED CHANGES

A. **Effect of the Proposed Changes.** It is important to understand that the goal of the FFADAA is to remove barriers to a fiduciary's access to electronic records and that the federal and state substantive rules of fiduciary, probate, trust, banking, security, and agency law remain unaffected by FFADAA. The act applies only to fiduciaries that act in compliance with their fiduciary powers. It distinguishes the authority of fiduciaries—which exercise authority subject to this act only on behalf of the user—from any other efforts to access the digital assets. Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.

This Act follows mirrors the Revised UFADAA because a uniform approach among states will provide certainty and predictability for courts, users, fiduciaries, and ISPs. The uniform act gives states precise, comprehensive, and easily accessible guidance on questions concerning fiduciaries' ability to access the electronic records of a decedent, protected person, principal, or a trust. Additionally, ISPs have participated in the redrafting of the Revised UFADAA and, presumably, find the proposed act to be acceptable.

The general goal of the FFADAA is to facilitate fiduciary access while respecting the privacy and intent of the user and concerns of the ISPs over federal privacy laws. It adheres to the traditional approach of trusts and estates law, which respects the intent of the user and promotes the fiduciary's ability to administer the user's property. With regard to the general scope of the act, the act's coverage is inherently limited by the definition of "digital assets." The act applies only to electronic records. The term does not include the underlying asset or liability unless it is itself an electronic record.

[11] For example, Facebook's Legacy Contact and Google's Inactive Account Manager.

B. The act is divided into **twenty sections**.

1. **Section 1** creates Chapter 740, Florida Statutes.

2. **Section 2** creates **740.001** which contains the short title of the Act.

3. **Section 3** creates **740.002** which contains general provisions and definitions, including those relating to the scope of the fiduciary's authority.

The definitions of "agent", "guardian", "court", "electronic", "fiduciary", "person", "personal representative", "power of attorney", "principal", "record", "trustee", "ward", and "will" are based on those found in applicable Florida law, such as the Florida Probate Code and Florida Powers of Attorney Act.

FloridaFADAAct	Florida Statutes
Section .002 Definitions	
(2) Agent	709.2102(1)
(6) Court	731.201(7)
(10) Electronic	709.2102(5)
(13) Fiduciary	739.102(6), 738.102 (4), 733.817, 518.10
(14) Guardian	744.604(6)
(17) Person	1.01(3)
(18) Personal Representative	731.201(28)
(19) Power of Attorney	709.2102(7)
(20) Principal	709.2102(9)
(21) Record	709.2102(13)
(24) Trustee	731.201(39)
(26) Ward	744.102(22)
(27) Will	731.201(40)

The other definitions are new for this Act, although the definition of digital service comes from the White House Digital Government Strategy: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf. The definition of "electronic communication" is from 18 U.S.C. §§ 2510(12); the definition of "electronic communication service" is drawn from 18 U.S.C. 2510(15); and the definition of "remote computing service" is adapted from 18 U.S.C. § 2711(2), to help ensure the Act's compliance with federal law.

A user includes any person who entered into a TOSA with a custodian, including a deceased individual who entered into the agreement during the individual's lifetime. A fiduciary is defined as a person, and a fiduciary can be a user when the fiduciary opens the account.

The Act includes a definition for "catalogue of electronic communications." This is designed to cover log-type information about an electronic communication such as the

email addresses of the sender and the recipient, and the date and time the communication was sent.

The term "content of an electronic communication" is adapted from 18 U.S.C. § 2510(8), but it refers only to information that is not readily accessible to the public because, if the information were readily accessible to the public, it would not be subject to the privacy protections of federal law under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 et seq. See S. Rep. No. 99-541, at 36 (1986). When the privacy protections of federal law under ECPA apply to the content of an electronic communication, the ECPA's legislative history notes the requirements for disclosure: "Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication."[12]

Example: X uses a Twitter account to send a message. If the tweet is sent only to other people who have been granted access to X's tweets, then it meets the Act's definition of "content of an electronic communication." But, if the tweet is completely public with no access restrictions, then it does not meet the Act's definition of "content of an electronic communication."

ECPA does not apply to private e-mail service providers, such as employers and educational institutions.[13]

A "custodian" includes any internet service provider as well as any other entity that provides or stores electronic data of a user. The term "carries" means engaging in the transmission or switching of electronic communications. See 47 U.S.C. § 1001(8). A custodian does not include most employers because an employer typically does not have a terms-of-service agreement with an employee. Any digital assets created through employment generally belong to the employer.

Example 1—Fiduciary access to an employee email account. D dies, employed by Company Y. Company Y has an internal email communication system, available only to Y's employees. D's personal representative, R, believes that D used Company Y's email system for some financial transactions that R cannot find through other means. R requests access from Company Y to the emails.

Company Y is not a custodian subject to the act. Under Section .101(7), a custodian must carry, maintain or store a user's digital assets. A user, in turn, is defined under Section .101(25) as someone who has entered into a terms-of-service agreement. Company Y, like most employers, did not enter into a terms-of-service agreement with D, so D was not a user.

[12] S. Rep. No. 99-541, at 37 (1986)).
[13] See 18 U.S.C. §2702(a)(2); James D. Lamm, Christina L. Kunz, Damien A. Riehl, & Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. 385, 404 (2014) (available at: http://goo.gl/T9jX1d).

Example 2—Employee of electronic-communication service provider. D dies, employed by Company Y. Company Y is an electronic-communication service provider. Company Y has an internal e-mail communication system, available only to Y's employees and used by them in the ordinary course of Y's business. D used the internal Company Y system. When not at work, D also used an electronic-communication service system that Company Y provides to the public. D's personal representative, R, believes that D used Company Y's internal e-mail system as well as Company Y's electronic-communication system available to the public to effectuate some financial transactions. R seeks access to both communication systems.

As is true in Example 1, Company Y is not a custodian subject to the act for purposes of the internal email system. The situation is different with respect to R's access to Company Y's system that is available to the public. Assuming that Company Y can disclose the communications under federal law, then Company Y must disclose the catalogue of electronic communications to R (unless the decedent opted out of disclosure) and will disclose the content of electronic communications if D consented to disclosure.

"Digital asset" includes products currently in existence and yet to be invented that are available only electronically. Digital assets include electronically-stored information, such as: 1) any information stored on a computer and other digital devices; 2) content uploaded onto websites, ranging from photos to documents; and 3) rights in digital property, such as domain names or digital entitlements associated with online games.[14] Both the catalogue and content of an electronic communication are covered by the term "digital assets."

The fiduciary's access to a record defined as a "digital asset" does not mean that the fiduciary is entitled to "own" the asset or otherwise engage in transactions with the asset. Consider, for example, funds in a bank account or securities held with a broker or other custodian, regardless of whether the bank, broker, or custodian has a brick-and-mortar presence. This Act affects records concerning the bank account or securities, but does not affect the authority to engage in transfers of title or other commercial transactions in the funds or securities, even though such transfers or other transactions might occur electronically. The Act reinforces the right of the fiduciary to access relevant electronic communications (subject to conditions) and the online account that provides evidence of ownership. Thus, an entity may not refuse to provide access to online records any more than the entity can refuse to provide the fiduciary with access to hard copy records.

The definition of "electronic communication" is that set out in 18 U.S.C. Section 2510(12):

"electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

[14] See Lamm, et al, supra, at 388.

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

The definition of "electronic-communication service" is drawn from 18 U.S.C. § 2510(15): "any service which provides to users thereof the ability to send or receive wire or electronic communications."

The definition of "remote computing service" is adapted from 18 U.S.C. § 2711(2): "the provision to the public of computer storage or processing services by means of an electronic communications system" and refers to 18 U.S.C. Section 2510(14), which defines an electronic communications system as: "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." The adaptation is to help ensure the Act's compliance with federal law. Electronic communication is a subset of digital assets and covers only the category of digital assets subject to the privacy protections of the ECPA. For example, material stored on a computer's hard drive is a digital asset but not an electronic communication.

A "fiduciary" under this chapter occupies a status recognized by Florida law, and fiduciaries' powers under the chapter are subject to the relevant limits established by other state laws.

An "online tool" means an electronic service that the custodian establishes and provides to a user, separate and apart from the TOSA, by which the user may direct disclosure or non-disclosure of digital assets to other persons.

The "terms-of-service agreement" ("TOSA") definition relies on the definition of "agreement" found in UCC § 1-201(3) and that found in UCC § 1-201(b) (3) ("the bargain of the parties in fact, as found in their language or inferred from other circumstances, including course of performance, course of dealing, or usage of trade"). It refers to any agreement that controls the relationship between a user and a custodian, even though it might be called a terms-of-use agreement, a click-wrap agreement, a click-through license, or a similar term. State and federal law determine capacity to enter into a binding terms-of-service agreement.

4. **Section 4** creates **740.003** which establishes the user's ability to direct disclosure of digital assets and the order of preference for the user's direction. A user's direction using an online tool prevails over an offline direction (such as a will, power of attorney, or trust) and over the TOSA so long as the online tool allows the user to modify or delete a direction at all times. Secondly, a user's direction in a will, trust, power of attorney or other record prevails over the TOSA regarding disclosure to a fiduciary. Thirdly, if a user provides no direction, the TOSA controls or other law controls if the TOSA are silent on fiduciary access.

5. **Section 5** creates **740.004** which establishes the effect on the terms of service agreement. This section clarifies that, unless it conflicts with a user's direction, TOSA are preserved and the fiduciary has no greater rights than the user. The fiduciary has the same authority as the user if the user were the one exercising the authority (note that, where the user has died, this means that the fiduciary has access as of the hour before the user's death).

6. **Section 6** creates **740.005** which establishes the procedure for disclosing digital assets. The custodian has three options for disclosing digital assets. First, the custodian may allow the fiduciary to access the user's account. Secondly, the custodian may allow the fiduciary to partially access the user's account if such limited access is sufficient to perform the necessary tasks. Thirdly, the custodian may provide the fiduciary with a "data dump" of all digital assets held in the account.

A custodian may assess a reasonable administrative charge for the cost of disclosing a user's digital assets. Deleted assets need not be disclosed. A request for some, but not all, of a user's digital assets need not be fulfilled if segregation is unduly burdensome. Instead, either party may petition the court for further instructions.

7. **Section 7** creates **740.006** which establishes the rights of personal representatives to the contents of electronic communications of a deceased user. A personal representative is not permitted to access the contents of a decedent's electronic communications absent consent by the user or direction by a court. The custodian may request a court order specifically identifying the account and finding consent. The subsection clarifies the difference between fiduciary authority over digital assets other than electronic communications protected by ECPA and authority over ECPA-covered electronic communications.

8. **Section 8** creates **740.007** which establishes the rights of personal representatives to other digital assets of a deceased user. A personal representative is permitted, however, to have access to all of the decedent's other digital assets (except the contents of electronic communications) unless the user prohibited disclosure or a court directs otherwise. The custodian may request a court order specifically identifying the account and finding that access is reasonably necessary for estate administration. This section establishes the default rule that the personal representative is authorized to access all of the decedent's digital assets other than material covered by the ECPA. The subsection clarifies the difference between fiduciary authority over digital assets other than electronic communications protected by ECPA and authority over ECPA-covered electronic communications.

9. **Section 9** creates **740.008** which establishes the rights of agents acting pursuant to a power of attorney to the contents of electronic communications of the principal. An agent acting pursuant to a power of attorney is permitted access to the contents of a principal's electronic communications if authority is expressly granted by the principal and not otherwise restricted by the principal or a court. The custodian may require specific identification of the account and evidence linking the account to the principal.

With respect to the contents of electronic communications, the agent must be specifically authorized by the principal to access the contents of the principal's electronic communications. Because a power of attorney contains the consent of the user, ECPA should not prevent the agent from exercising authority over the content of electronic communications. There should be no question that an explicit delegation of authority in a power of attorney constitutes authorization from the user to access digital assets, and provides "lawful consent" to allow disclosure of electronic communications from an electronic communication service or a remote computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The uniform law commissioners considered whether the authority over digital assets and electronic communications should be a default power. They decided that the power to access the contents of electronic communications must be expressly granted, because when expressed and not default, it satisfies the lawful consent requirement of ECPA. The agent has default authority over other digital assets under the Act.

Federal law distinguishes between the permissible disclosure of the "contents" of a communication, covered in 18 U.S.C. § 2702(b), and of "a record or other information pertaining to a" subscriber or customer, covered in 18 U.S.C. § 2702(c).[15] Content-based material can, in turn, be divided into two types of communications: those received by the user and those sent. Material when the user is the "addressee or intended recipient" can be disclosed either to that individual or to an agent for that person, 18 U.S.C. § 2702(b)(1), and it can also be disclosed to third parties with the "lawful consent" of the addressee or intended recipient. 18 U.S.C. § 2702(b)(3). Material for which the user is the "originator" can only be disclosed to third parties with the user's "lawful consent." 18 U.S.C. § 2702(b)(3). (Note that, when the user is the addressee or intended recipient, material can be disclosed under either § 2702(b)(1) or (b)(3), but that when the user is the originator, lawful consent is required.)

By contrast to content-based material, non-content material can be disclosed not only with the lawful consent of the user but also to any person other than a governmental entity (which would presumably include fiduciaries). This information includes material about any communication sent, such as the addressee, sender, date/time, and other subscriber data, what this Act defines as the "catalogue of electronic communication". (Further discussion of this issue and examples are set out in the comments to Section .1401, *infra*.)

10. **Section 10** creates **740.009** which establishes the rights of agents acting pursuant to a power of attorney to other digital assets of the principal. An agent acting pursuant to a power of attorney granting specific authority over digital assets or general authority to act on behalf of a principal is permitted access to the catalogue of a principal's electronic communications and any other digital assets (except the contents

[15] See Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105 (2009).

of electronic communications), unless otherwise directed by the principal, a court, or the power of attorney. The custodian may require specific identification of the account and evidence linking the account to the principal. This section establishes that the agent has default authority over the principal's digital assets and the records, other than the contents, of the principal's electronic communications. When the principal does not want the agent to exercise this authority, then the power of attorney must explicitly prevent an agent from doing so.

11. **Section 11** creates **740.01** which establishes the rights of trustees when the trustee is the original user. A trustee that is an original user may access any digital asset—including catalogue and content of electronic communications—held by the trust unless that is contrary to the terms of the trust or otherwise directed by a court. Access to digital assets, including the contents of the electronic communications, is presumed with respect to assets for which the trustee is the initial user. A trustee may have title to digital assets and electronic communications when the trust itself becomes the user of a digital asset held by the trust, and when the trustee becomes a user for trustee business. The underlying trust documents and the Florida Trust Code will supply the allocation of responsibilities between and among trustees.

12. **Section 12** creates **740.02** which establishes the rights of trustees to contents of electronic communications held in trust when the trustee is not the original user. A trustee that is not an original user may access the content of an electronic communication in an account of the trust if the trust includes consent to such disclosure, unless prohibited by the user, the trust instrument, or a court. The custodian may require specific identification of the account and evidence linking the account to the trust.

Sections .02 and .03 address situations involving either an inter vivos transfer of a digital asset into a trust or transfer via a pour-over will of a digital asset into a trust. In those situations, a trustee becomes a successor user when the settlor transfers a digital asset into the trust. Nonetheless, sections .02 and .03 distinguish between the catalogue and contents of electronic communications in case there are any questions about whether the form in which property – transferred into a trust - is held constitutes lawful consent. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization, and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The underlying trust documents and the Florida Trust Code will supply the allocation of responsibilities between and among trustees.

13. **Section 13** creates **740.03** which establishes the rights of trustees to other digital assets held in trust when the trustee is not the original user. A trustee that is not an original user may access the catalogue of electronic communications and any digital assets (excluding the content of electronic communication) in an account of the trust, unless prohibited by the user, the trust instrument, or a court. The custodian may require specific identification of the account and evidence linking the account to the trust. The underlying trust documents and the Florida Trust Code will supply the allocation of responsibilities between and among trustees.

14. **Section 14** creates **740.04** which establishes the rights of guardians.

A guardian is not permitted to access the contents of a ward's electronic communications absent consent by the ward. A guardian is permitted, however, to access all of the ward's other digital assets (except the contents of electronic communications) pursuant to letters of guardianship or a court order, unless directed otherwise by a court or by the user. The custodian may request specific identification of the account and evidence linking the account to the ward. The custodian may suspend or terminate an account for good cause if requested by the guardian of the property.

This section establishes that the guardian must be specifically authorized (not implicitly authorized) to access the ward's digital assets and electronic communications. The requirement for express authority over digital assets does not limit the fiduciary's authority over the underlying "bricks and mortar" assets, such as a bank account. As a legislative enacting matter, the meaning of the term "hearing" will vary, depending on a state's procedures.

Section .04 is comparable to Sections .006 and .007. It responds to the concerns of ISPs who believe that the Act should be structured to clarify the difference between fiduciary authority over digital assets other than electronic communications protected by federal law (the ECPA) and fiduciary authority over ECPA-protected electronic communications. Consequently, this Act sets out procedures that cover all digital assets as well as the catalogue of electronic communications (logs and records) that providers may release without consent under ECPA and addresses ECPA-covered communications.

The guardian must exercise authority in the best interests of the ward pursuant to Chapter 744.

15. **Section 15** creates **740.05** which contains provisions relating to the rights and duties of the fiduciary to access digital assets. In exercising its responsibilities, the fiduciary is subject to the duties and obligations established pursuant to Florida law and is liable for breach of those duties.

This issue concerning the parameters of the fiduciary's authority potentially arises in two situations: 1) the fiduciary obtains access to a password directly from the user, as would be true in various circumstances such as for the trustee of an inter vivos trust or someone who has stored passwords with a digital locker and those passwords are then transmitted to the fiduciary; and 2) the fiduciary has obtained access pursuant to this Act.

The fiduciary does not, however, obtain power over any digital assets if that property was illegally obtained by the user. Note that even if the digital asset were illegally obtained by the user, the fiduciary would still need access in order to handle that asset appropriately. There may, for example, be tax consequences that the fiduciary would be obligated to report.

Finally, the fiduciary has the same responsibilities as the user more generally. For example, a fiduciary cannot delete an account if this would be fraudulent. Similarly, if

the user could challenge provisions in a terms-of-service agreement, then the fiduciary is similarly able to do so.[16]

Subsection (2) is designed to establish that the fiduciary is authorized to exercise control over digital assets in accordance with other applicable laws. A fiduciary's control over a digital asset is not equivalent to a transfer of ownership or a laundering of illegally obtained material. For example, where the user has an online securities account or has a game character and in-game property associated with an online game, then the fiduciary's ability to sell the securities, the game character, or the in-game property is controlled by traditional probate law. The act is only granting access in the sense of enabling the fiduciary to do electronically what the user could have done electronically. Thus, if a TOSA precludes online transfers, then the fiduciary is unable to make those transfers electronically as well.

Example – Fiduciary control over a digital asset. D dies with a will disposing of all D's assets to D's spouse, S. E is the personal representative for D's estate. D left a bank account, for which D only received online statements, and a blog.

E as personal representative of D's estate has access to both of D's accounts and can request the passwords from the custodians of both accounts. If D's agreement with the bank requires that transferring the underlying title to the account be done in person, through a hard copy signed by the user and the bank manager, then E must comply with those procedures (signing as the user) and cannot transfer the funds in the account electronically. If the TOSA for the blog permitted D to transfer the blog electronically, then E can make the transfer electronically as well.

The subsection clarifies that the fiduciary is "authorized" under the two federal statutes that prohibit unauthorized access to computers and computer data, the SCA and the CFAA,[17] as well as pursuant to any comparable state laws criminalizing unauthorized access.[18] The language mirrors that used in Title II of the ECPA, known as the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*

The Stored Communications Act contains two potentially relevant prohibitions.

---

[16] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013).

[17] Stored Communications Act, 18 U.S.C. § 2701 *et seq*. (2006); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. (2006); *see, e.g.,* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Allan D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295 (2012).

[18] *See Computerized Hacking and Unauthorized Access States Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 21, 2009), http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx; Christina Kunz, Peter Rademacher & Lucie O'Neill, 50 State Survey of Unauthorized Access (2012) (on file with the Committee and available on the Google Drive); James D. Lamm, et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. __ (2013), http://lawreview.law.miami.edu/wp-content/uploads/2011/12/The-Digital-Death-Conundrum-How-Federal-and-State-Laws-Prevent-Fiduciaries-from-Managing-Digital-Property.pdf.

(a) 18 U.S.C. § 2701(a), which concerns access to the digital assets, makes it a crime 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." Thus, someone who has authorization to access the facility is not engaging in criminal behavior. Moreover, 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."[19]

(b) 18 U.S.C. § 2702, "Voluntary disclosure of customer communications or records," concerns actions by the service provider. It 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 unless disclosure is made (among other exceptions) "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient" or "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."[20] The statute permits disclosure of "customer records" that do not include content, either with lawful consent from the customer or "to any person other than a governmental entity."[21] Thus, unlike the contents, the provider is permitted to disclose the non-content "records" of the electronic communications to anyone except the government, and may disclose to the government with the customer's lawful consent or in certain emergencies.

The Computer Fraud and Abuse Act prohibits unauthorized access to computers. 18 U.S.C. § 1030. Like the SCA, the CFAA similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a).

Florida laws prohibit unauthorized access. See Chapters 815 and 934, Florida Statutes.

By defining the fiduciary as an authorized user, the fiduciary has authorization to access the files under the *first* section of the SCA, 18 U.S.C. § 2701, as well as under the CFAA. Moreover, this language should be adequate to avoid liability under the Florida unauthorized access laws. The "lawful consent" of the originator/subscriber must be specifically granted by the user so that the provider can voluntarily disclose the files pursuant to the *second* relevant provision of the SCA, 18 U.S.C. § 2702.

However, an online tool by which a user has made an affirmative choice, separate from the user's assent to other provisions of the terms-of-service agreement, to grant or to limit a fiduciary's access to the user's digital assets is not voided by this Act and will supersede any contrary provision in a will or trust. (*See* Example 5).

Subsections (2) and (3) reinforce the concept that the fiduciary "steps into the shoes" of the user, with no more – and no fewer – rights. For example, the TOSA

[19] 18 U.S.C. §§ 2701(a), (c)(2).
[20] 18 U.S.C. § 2702(b)(1), (3) (emphasis added).
[21] 18 U.S.C. § 2702(c)(2) and (6).

controls the rights of the user (settlor, principal, incapacitated person, decedent). The Act does not permit the user's fiduciary to override the TOSA in order to make a digital asset or collection of digital assets "descendible," although it does preserve the rights of the fiduciary to make the same claims as the user.[22]

Subsections (4) and (5) are designed to clarify that the fiduciary is authorized to access digital assets stored on equipment of the decedent, ward, principal, or settlor, thereby superseding Florida laws on unauthorized access to the equipment. For criminal law purposes, this clarifies that the fiduciary is authorized to access all of the user's digital assets, whether held locally or remotely.

Example 1 – Access to digital assets by personal representative. D dies with a will that is silent with respect to digital assets. D has a bank account for which D received only electronic statements, D has stored photos in a cloud-based Internet account, and D has an e-mail account with a company that provides electronic-communication services to the public. The personal representative of D's estate needs access to the electronic bank account statements, the photo account, and e-mails.

The personal representative of D's estate has the authority to access D's electronic banking statements and D's photo account, which both fall under the Act's definition of a "digital asset," unless D opted out or a court directs otherwise. This means that, if these accounts are password-protected or otherwise unavailable to the personal representative, then the bank and the photo account service must give access to the personal representative when the request is made in accordance with Section .701. The custodian may request a court order specifically identifying the account and finding that access is reasonably necessary for estate administration. If the TOSA permits D to transfer the accounts electronically, then the personal representative of D's estate can use that procedure for transfer as well.

The personal representative of D's estate is also able to request that the e-mail account service provider grant access to e-mails sent or received by D; the Act and ECPA permit the service provider to release the catalogue to the personal representative. The service provider will not provide the personal representative access to the content of an electronic communication sent or received by D if D did not consent to disclose the content. The service provider may request a court order specifically identifying the account and finding consent. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not a custodian providing electronic communication services to the public or providing a remote-computing service to the public.

Example 2 – Access to digital assets by guardian. C is seeking appointment as

[22] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013); David Horton, *Indescendibility*, 102 Calif. L. Rev. __ (forthcoming 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311506.

the guardian of the property for P. P has a bank account for which P received only electronic statements, P has stored photos in a cloud-based Internet account, and P has an e-mail account with a company that provides electronic communication services to the public. C needs access to the electronic bank account statements, the photo account, and e-mails.

Without a court order that explicitly grants access to P's digital assets, including the catalogue of electronic communications, C has no authority pursuant to this Act to access the electronic bank account statements, the photo account, or the e-mails. The contents of the e-mail account may not be disclosed without the express consent of the Ward (granted prior to incapacity). The service provider may suspend or terminate an account for good cause if requested by the guardian. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not a custodian providing electronic communication services to the public or providing a remote-computing service to the public.

Example 3 – Access to digital assets by agent. X creates a power of attorney designating A as X's agent. The power of attorney expressly grants A authority over X's digital assets, including the content of an electronic communication. X has a bank account for which X receives only electronic statements, X has stored photos in a cloud-based Internet account, and X has a game character and in-game property associated with an online game. X also has an e-mail account with a company that provides electronic-communication services to the public.

A has the authority to access X's electronic bank statements, the photo account, the game character and in-game property associated with the online game, all of which fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to A as X's agent, then the bank, the photo account service provider, and the online game service provider must give access to A when the request is made in accordance with Section .009. The custodian may require specific identification of the account and evidence linking the account to the principal. If the TOSA permits X to transfer the accounts electronically, then A as X's agent can use that procedure for transfer as well.

As X's agent, A is also able to request that the e-mail account service provider grant access to e-mails sent or received by X. This Act permits the service provider to release the catalogue and, because the power of attorney expressly granted authority over the contents of electronic communications sent or received by X, the service provider also must provide A access to the content of an electronic communication. The custodian may require specific identification of the account and evidence linking the account to the principal. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not a custodian providing electronic communication services to the public or providing a remote-computing service to the public.

Example 4 – Access to digital assets by trustee. T is the trustee of a trust

established by S. As trustee of the trust, T opens a bank account for which T receives only electronic statements. S transfers into the trust to T as trustee (in compliance with a TOSA) a game character and in-game property associated with an online game and a cloud-based Internet account in which S has stored photos. S also transfers to T as trustee (in compliance with the TOSA) an e-mail account with a company that provides electronic-communication services to the public.

T is an original user with respect to the bank account that T opened, and T has the ability to access the electronic banking statements. T, as successor user to S, may access the game character and in-game property associated with the online game and the photo account, which both fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to T as trustee, then the bank, the photo account service provider, and the online game service provider must give access to T when the request is made in accordance with Section .03. If the TOSA permits the user to transfer the accounts electronically, then T as trustee can use that procedure for transfer as well. The custodian may require specific identification of the account and evidence linking the account to the trust.

T as successor user of the e-mail account for which S was previously the user is also able to request that the e-mail account service provider grant access to e-mails sent or received by S. The Act permits the service provider to release the catalogue, unless otherwise directed by the user, the trust, or a court. The service provider also must provide T access to the content of an electronic communication sent or received by S if the trust includes consent to disclosure of the contents of electronic communications to the trustee. The custodian may require specific identification of the account and evidence linking the account to the trust. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not a custodian providing electronic communication services to the public or providing a remote-computing service to the public.

Example 5 – Access notwithstanding terms in a TOSA. D, who is domiciled in Florida, dies. D was a professional photographer who stored valuable digital photos in an online storage account provided by C. P is appointed by a court in Florida to administer D's estate. P needs access to D's online storage account to inventory and appraise D's estate assets and to file D's estate tax return. During D's lifetime, D entered into a TOSA with C for the online storage account. The choice-of-law provision selects the law of state Y to govern the contractual rights and duties under the TOSA. A provision of the TOSA prohibits fiduciary access to the digital assets of a user, but, using the custodian's online tool, separate from D's assent to other provisions of the TOSA, D designated P to have access to his account. FFADAA has been enacted but no similar law has been enacted by state Y. Because of D's direction using an online tool to grant access to P, the custodian must grant P access to D's assets, even though the TOSA selected the law of state Y to govern the contractual rights and duties under the TOSA.

16. **Section 16** creates **740.06** which addresses compliance and grants immunity to custodians.

Subsection (1) establishes 60 days as the appropriate time for compliance. If the custodian fails to comply, then the fiduciary may apply to the court for an order directing compliance and finding that compliance does not violate 18 U.S.C. § 2702.

Subsection (4) establishes that, in the situation of a joint account, a custodian may deny a fiduciary's request for disclosure or account termination if the custodian is aware of any lawful access to the account following the fiduciary's request for access.

This section establishes that custodians are protected from liability when they act, or fail to act, in accordance with the procedures of this Act and in good faith. The types of actions covered include disclosure as well as transfer of copies.

17. **Section 17** creates **740.07** which establishes the relation with the Electronic Signatures in Global and National Commerce Act.

18. **Section 18** creates **740.08** which establishes the applicability of this Act. This Act applies in situations in which a decedent dies testate or intestate, as well as a guardianship, a power of attorney, and a trust, and to a custodian if the user resides in Florida. This Section clarifies that the Act does not apply to a fiduciary's access to an employer's internal email system. The treatment of digital assets of an employer used by an employee in the ordinary course of the employer's business is discussed in Section 3 establishing 740.002.

This Act does not change the substantive rules of other law, such as agency, banking, guardianship, contract, copyright, criminal, fiduciary, privacy, probate, property, security, trust, or other applicable law except to vest fiduciaries with authority, according to the provisions of this Act, to access, control, or copy digital assets of a decedent, ward, principal, settlor, or trustee.

19. **Section 19** creates **740.09** which establishes the severability of the provisions of the act.

20. **Section 20** establishes the effective date.

IV. FISCAL IMPACT ON STATE AND LOCAL GOVERNMENTS

The proposal does not have a fiscal impact on state or local governments. In fact, it should decrease the risk of unauthorized access to digital assets from the fiduciaries appointed by users and would provide certainty and predictability for courts, users, fiduciaries, and Internet service providers.

V. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR

The proposal does not have a direct economic impact on the private sector.

VI. CONSTITUTIONAL ISSUES

There appear to be no constitutional issues raised by this proposal.

VII. OTHER INTERESTED PARTIES

Criminal Law Section, State law enforcement and state attorney offices who track and enforce privacy and cyber crimes.

Florida Bankers Association

Business Law Section

Trial Lawyers Association

Exhibit D

See attached My Digital Audit Form
(Courtesy of James D. Lamm, Esq.)

My Digital Audit:
Passwords, Online Accounts, & Digital Property

Voicemail & Home Security Systems

Name: _____

Home address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Security company & phone #: _____ _____

Security system password: _____

Vacation home address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Security company & phone #: _____ _____

Security system password: _____

Business address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Personal cell phone # & password: _____ _____

Voicemail # & password: _____ _____

Business cell phone # & password: _____ _____

Voicemail # & password: _____ _____

Safe/lockbox location & combination: _____ _____

Safe/lockbox location & combination: _____ _____

Other: _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Computer Passwords

Home computer #1 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Home computer #2 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Home computer #3 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Office computer #1 description: _____

Username & password: _____ _____

Office computer #2 description: _____

Username & password: _____ _____

Other devices: _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

E-Mail Accounts

E-Mail Provider	E-Mail Address	Password
Home e-mail:		
Work e-mail:		
Microsoft Outlook/Hotmail:		
Yahoo! Mail:		
Google Gmail:		
Other:		

Social Networking Accounts

Service	Username	Password
Facebook:		
LinkedIn:		
Google+		
MySpace:		
Twitter:		
Foursquare:		
Other:		

Instant Messaging, Chat, & Videoconference Accounts

Service	Username	Password
Skype:		
AOL Instant Messenger:		
Yahoo! Messenger:		
ICQ:		
Google Talk:		
Jabber:		
Other:		

Financial Accounts

Intuit Quicken software password: _____

Mint.com username & password: _____ _____

PersonalCapital.com username & password: _____ _____

PowerWallet.com username & password: _____ _____

Tax preparation software password: _____

Bank #1 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Bank #2 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Brokerage #1 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Brokerage #2 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Credit card #1 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #2 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Financial Accounts (Continued)

Credit card #3 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #4 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #5 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Other: _____ _____

Domain Names, Web Pages, & Blogs

Domain Name & Registrar/Host	**Username**	**Password**

Online Storage Accounts

Website	**Username**	**Password**
Apple iCloud:		
Dropbox:		
Google Drive:		
Microsoft OneDrive:		
Other:		

Online Shopping & Auction Accounts

Website	**Username**	**Password**
Amazon:		
Barnes & Noble:		
Craigslist:		
Ebay:		
PayPal:		
Western Union:		
Other:		

Video Games & Virtual Worlds

Website	**Username**	**Password**

Intellectual Property

Website or Other Location	**Username**	**Password**
Instagram:		
Flickr:		
Photobucket:		
SmugMug:		
YouTube:		
Vimeo:		

Digital Music, eBook, Video and Other Media Accounts

Website	**Username**	**Password**
Amazon Kindle/Prime:		
Apple iTunes:		
Barnes & Noble Nook:		
Hulu:		
Netflix:		
YouTube:		
Other:		

Other Online Accounts

Website	**Username**	**Password**

Other Online Accounts

Website	Username	Password

Exhibit E

Sample language for a durable power of attorney*:

I authorize my Agent to access and deal freely with any digital assets[10] I own or in which I am an account holder or authorized user, either in my own name or jointly with anyone, including but not limited to online accounts relating to email, banks, brokerage firms, Internet service providers, retail vendors, utilities, mutual funds and the like; to open new accounts and close accounts as my Agent determines is necessary or advisable and in my best interests; and to transfer funds among my online accounts as my Agent deems necessary or advisable.

In order to exercise the authority granted above, I further authorize my Agent:

- **(a) To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device; and**
- **(b) To take such actions as necessary, including employing agents to assist my Agent in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, user name, or authorization in order to access any digital device or digital asset of mine.**

My Agent shall NOT have access to the following digital assets/electronic communications:

_____
_____.

Except as specifically limited above, I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Agent any electronically stored information of mine; the contents of any electronic communications sent or received by me; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Fiduciary Access to Digital Assets Act, the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law. An individual or entity may accept a copy of this original authorization as though it were an original document.

***This grant of power is very broad. To the extent the principal desires to limit the Agent's authority, those limitations would need to be added to the power of attorney document.**

---

[10] **"Digital asset" means an electronic record in which the principal has a right or interest, or as otherwise defined in Chapter 740, Florida Statutes. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record**.

Exhibit F

Sample language for a will*:

I grant to my Personal Representative full power and authorization to access and deal freely with any digital assets[11] in my estate. "Digital assets" include but are not limited to online accounts relating to email, banks, brokerage firms, Internet service providers, retail vendors, utilities, mutual funds and the like. The Personal Representative may exercise all power and authority over my digital assets that an owner and/or account holder or authorized user of the digital asset would have. In order to exercise the authority granted above, I further authorize the Personal Representative:

(a) To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device;
(b) To take such actions as necessary, including employing agents to assist in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, user name, or authorization in order to access any digital device or digital asset of mine; and
(c) To securely/permanently delete the following digital assets: _____ _____.

My Personal Representative shall NOT have access to the following digital assets/electronic communications:

_____ _____.

Except as specifically limited above, I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Personal Representative any electronically stored information of mine; the contents of any electronic communications sent or received by me; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Fiduciary Access to Digital Assets Act, the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law.

***This grant of power is very broad. To the extent the testator desires to limit the Personal Representative's authority, those limitations would need to be inserted above.**

---

[11] **"Digital asset" means an electronic record in which the decedent has a right or interest, or as otherwise defined in Chapter 740, Florida Statutes. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.**

Exhibit G

Sample language for a trust*:

I grant to my Trustee full power and authorization to access and deal freely with any digital assets[12] in my trust estate. "Digital assets" include but are not limited to online accounts relating to email, banks, brokerage firms, Internet service providers, retail vendors, utilities, mutual funds and the like. The Trustee may exercise all power and authority over my digital assets that an owner and/or account holder or authorized user of the digital asset would have. In order to exercise the authority granted above, I further authorize the Trustee:

(a) To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device, if the digital device has been transferred into the trust;
(b) To take such actions as necessary, including employing agents to assist the Trustee, in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, username, or authorization in order to access any digital device or digital asset of mine;
(c) Upon my death to securely/permanently delete the following digital assets:
_____
_____.

My Trustee (or Successor Trustee if the Settlor is the original sole trustee of the Trust) shall NOT have access to the following digital assets/electronic communications:
_____
_____.

Except as specifically limited above, I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Trustee any electronically stored information of mine; the contents of any electronic communications sent or received by me; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Fiduciary Access to Digital Assets Act, the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law.

***This grant of power is very broad. To the extent the settlor desires to limit the Trustee's authority, those limitations would need to be inserted above.**

---

[12] **"Digital asset" means an electronic record in which the settlor has a right or interest, or as otherwise defined in Chapter 740, Florida Statutes. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.**

Exhibit H

Guidance for Managing Deceased Accounts

Reinstating Membership Rewards® points

The Membership Rewards® points accumulated by a deceased Cardmember may be reinstated to a new basic account or be redeemed by the estate of the deceased Cardmember.

If you are already an Additional Cardmember on the deceased account:

1. Assume ownership of the account, for details please see Taking over the account.
2. Call us and request to reinstate the points to your new account. Contact our dedicated Membership Rewards team at **1-800-297-3276** Monday through Friday from 9:00 am to 12:00 am EST and Saturday between 10:00 am and 6:30 pm EST.

If you have chosen not to assume ownership of the account or are not an additional Cardmember:

1. The Executor of the Estate must send a formal written request to the Membership Rewards® Correspondence Unit for the distribution of the points. The written request must include:
   - The name and position of the Executor of the estate
   - Name(s) of individual(s) designated/entitled to the Membership Rewards® points
   - Specific redemptions to process (e.g. 50,000 to Delta, 10,000 Home Depot)
   - A copy of the death certificate
2. The written request should be addressed to:
   Membership Rewards® Correspondence Unit
   American Express Membership Rewards
   PO Box 297813
   Ft Lauderdale, FL 33329-7813

Please note accrued points in Membership Rewards® will be forfeited immediately upon cancellation of all Cards so please make sure to redeem points before cancelling the account. Depending on the Card, the estate might only be able to redeem points within a certain time frame.

To learn about our Membership Rewards® click here.

When you are ready, please call us at **1-800-266-7064** Monday through Friday from 8:00 am to 9:00 pm EST and Saturday between 10:00 am and 6:00 pm, Saturday EST. For Corporate Cards, please contact your company's Program Administrator.

DECEASED ACCOUNT MANAGEMENT