Digital Assets Legislative Update (Now Snapchat That!)

Presented at the SunTrust Bank
Private Wealth Management Luncheon

October 20, 2015

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

Digital Assets Update

I. What are Digital Assets?

"Digital assets" are electronic records that are transmitted or stored on digital devices such as smartphones and computers. 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) Digital currency such as bitcoins or credits with online vendors such as iTunes; and
(j) Artistic content such as photographs.

For the purposes of this outline, it makes sense at the outset to define terms for discussion. This presentation 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 a proposed revised Florida Fiduciary Access to Digital Assets Act.[1] These definitions will likely be contained in legislation proposed by the Florida Senate and House for the 2016 legislative session. In this outline I will refer to the revised Florida Fiduciary Access to Digital Assets Act as "the Proposed Act."

[1] The revised legislation referenced will update the original Florida Fiduciary Access to Digital Assets Act that was part of 2015 Florida legislative efforts under SB 102 (Hukill) and HB 313 (Fant). The 2015 legislative efforts did not result in passage of the original act.

Here are some definitions from the Proposed Act:

a. "Account" means an arrangement under a terms-of-service agreement in which the custodian holds one or more digital assets of the user or provides goods or services to the user.

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. "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.

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

f. "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.[2]

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

g. "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.

h. "Terms of service agreement" means an agreement that controls the relationship between a user and a custodian.[3]

i. "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

[3] Terms of service agreements 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.

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 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 Face With Regard to Digital Assets

The biggest problem is lack of defined right of access for fiduciaries. The Florida Probate Code, and Florida law in general, does not mention digital assets, does not define these assets, and does not contain clearly applicable rules governing access to them by fiduciaries.

More importantly, access to digital assets creates a minefield where fiduciaries can unknowingly violate both federal and state criminal law regarding hacking and privacy. Virtually none of these criminal laws have a provision for fiduciary access.

Fiduciaries also can run afoul of TOS provisions in attempting to access digital assets. One internet service provider (Google) has created a third-party access mechanism for U.S. customers, but the author is unaware of other such provider mechanisms for third parties.

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.

V. What Law Applies to Digital Assets?

A. Florida Law

Florida law does not specifically define or address digital assets or digital information, other than in a criminal law context.[4] To the extent Florida probate, guardianship, and trust law applies to digital assets it is now unclear how that law may be preempted or in conflict with relevant federal and Florida statutes that relate to issues such as privacy and hacking. There are no Florida cases relating to fiduciary access to digital assets or post-mortem administration of digital assets.

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

[4] F.S. Secs. 815.01-07 Computer-Related Crimes. For example, s. 815.06(2)(a) states – "A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized;…." There is no explicit statutory language authorizing fiduciary access. The offense is a third-degree felony.

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*, 83 Mass.App.Ct. 565 (2013)(where there have been more than 7 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. A Proposed Solution – Florida Fiduciary Access to Digital Assets Act

The Proposed Act is designed to be a stand-alone act rather than legislation that addresses digital assets in piecemeal fashion in the Probate Code, the Trust Code, and so forth. The Proposed Act is divided into 12 main sections. Section 1 contains definitions of terms. Digital assets are defined broadly. Section 2 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. Section 3 provides for treatment of terms-of-service agreements. Section 4 provides procedures for the disclosure of digital assets generally. Sections 5-8 establish the rights of personal representatives, agents acting pursuant to a power of attorney, trustees, and guardians. Sections 9-10 impose fiduciary duties and provide for the responsibilities of a person acting in a fiduciary capacity and require compliance of a custodian. Section 11 provides for immunity from liability for a custodian and its officers, employees, and agents acting in good faith in compliance. The final portions of the Act, Section 12 collectively, address miscellaneous issues, including the effective date of the act which would likely be July 1, 2016 if enacted.

The Proposed Act is a solution to the bigger roadblocks to fiduciary access. The Proposed Act does 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 Proposed Act is inapplicable to digital assets of employers used by employees in the ordinary course of the employer's business.

The Proposed 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 Proposed Act makes only governs access to digital assets. The underlying ownership and title of assets is not changed by the Proposed Act. Asset title and ownership would be governed by existing law.

The Proposed 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.

The Proposed Act 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 Proposed Act.[5]

[5] 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 B to these materials. The Proposed Act would have the same description as the Revised UFADAA in the table.

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.

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 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 C.[6]

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.

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.

---

[6] 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.

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

Sample forms[7] relating to fiduciary powers are set forth in Exhibits D (for powers of attorney), E (for wills), and F (for trusts). ***Please use caution with regard to any review of these 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.***

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.

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

A. Select Appropriate Personal Representatives and Empower Them

[7] 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.

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 E 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 and until the Proposed Act passes, the personal representative should seek a specific court order giving the personal representative 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 and Administering These Assets

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 digital currency such as bitcoins) 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.

Regular email accounts will normally grant a personal representative access to a catalog of emails sent and received (to, from, subject, date, etc.) but not the contents of the emails themselves (this varies). 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 e-mail 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.

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.

Under current law, filing lawsuits to get information and gain control over digital assets is a strategy with significant drawbacks. Lawsuits are slow and expensive and you likely will run into legal problems such as the SCA issues raised in the *Ajemian* case. In addition, litigation to gain access to employer email accounts is unlikely to be successful for a variety of reasons.

Unless the Proposed Act passes, the personal representative should only use the decedent's passwords on a very temporary basis (if at all) until they can be legally changed for the personal representative's use or access is otherwise provided. As discussed above, use of the decedent's passwords may be deemed legally unauthorized.

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.

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 G.

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.

D. 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.

Digital currency has a monetary value which can be determined online depending upon the type of currency involved.

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 comparable sales, cash flows, auction value, etc. Since this is a new area this is easier said than done. Comparable sales are hard to find and historical costs are hard to determine in this area. This is an area where use of an expert to appraise the property will be helpful.

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.

E. 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 device itself so that is not recommended. See *Capital Records v. ReDigi*, 2013 WL 1286134 (S.D.N.Y. 2013).

Exhibit A

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 B

COMPARISON OF THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (ORIGINAL UFADAA), THE PRIVACY EXPECTATIONS AFTERLIFE AND CHOICES ACT (PEAC ACT), AND THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (REVISED UFADAA)

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Estate representative's access to the *content of a decedent's electronic communications*.	Permitted unless the decedent opted out while alive.	Not permitted unless a court finds that the decedent consented to disclosure and the estate indemnifies the custodian. The request must specifically identify the account.	Not permitted unless the decedent consented to disclosure. Custodian may request a court order specifically identifying the account and finding consent. Indemnification not required.
Estate representative's access to *other digital assets* of a decedent.	Permitted unless the decedent opted out while alive.	Unless the decedent opted out, access to one years' worth of records permitted with a court order only if relevant to resolve fiscal assets of the estate.	Permitted unless the decedent opted out or the court directs otherwise. Custodian may request a court order specifically identifying the account and finding that access is reasonably necessary for estate administration.
Guardian's access to the *content of a ward's electronic communications*.	Permitted if access ordered by the court.	Not addressed.	Custodian need not disclose contents without the express consent of the ward, but may suspend or terminate an account for good cause if requested by the guardian.
Guardian's access *to other digital assets* of a ward.	Permitted if access ordered by the court.	Not addressed.	Permitted if authorized by the guardianship order. Custodian may require specific identification of the account and evidence linking the account to the ward.
Agent's access to the *content of a principal's electronic communications*.	Permitted if expressly authorized by the principal.	Not addressed.	Permitted if expressly authorized by the principal. Custodian may require specific identification of the account and evidence linking the account to the principal.

COMPARISON OF THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (ORIGINAL UFADAA), THE PRIVACY EXPECTATIONS AFTERLIFE AND CHOICES ACT (PEAC ACT), AND THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (REVISED UFADAA)

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Agent's access to *other digital assets.*	Permitted under a grant of general or specific authority.	Not addressed.	Permitted under a grant of general or specific authority. Custodian may require specific identification of the account and evidence linking the account to the principal.
Trustee's access to the *contents of electronic communications* of a trust account.	Permitted unless prohibited by the user, trust, or court.	Not addressed.	Permitted when trustee is the original user. Also permitted when the trustee is not the original user if authorized by the trust. Custodian may require specific identification of the account and evidence linking the account to the trust.
Trustee's access to *other digital assets* of the trust.	Permitted unless prohibited by the user, trust, or court.	Not addressed.	Permitted unless prohibited by the user, trust, or court. Custodian may require specific identification of the account and evidence linking the account to the trust.

COMPARISON OF THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (ORIGINAL UFADAA), THE PRIVACY EXPECTATIONS AFTERLIFE AND CHOICES ACT (PEAC ACT), AND THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (REVISED UFADAA)

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Effect of boilerplate term-of-service prohibiting fiduciary access.	A blanket prohibition on fiduciary access is void as against public policy.	Not specifically addressed, but terms-of-service arguably enforceable by the reference to "other applicable law" (i.e. contract law) in Sec. 3(c).	Three tiered approach: 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. 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.
Effect of other terms-of-service.	Not addressed.	Recipient has no greater rights than the user.	Unless they conflict with a user's direction, terms-of-service are preserved and the fiduciary has no greater rights than the user.

COMPARISON OF THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (ORIGINAL UFADAA), THE PRIVACY EXPECTATIONS AFTERLIFE AND CHOICES ACT (PEAC ACT), AND THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (REVISED UFADAA)

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Procedure for disclosing digital assets.	Not addressed, but use of the term "access" throughout the act arguably contemplates the fiduciary logging on to the user's account.	Provider not required to allow a requesting party to assume control of a deceased user's account.	The custodian has three options for disclosing digital assets: 1. Allow the requestor to access the user's account. 2. Allow the requestor to partially access the user's account if sufficient to perform the necessary tasks. 3. Provide the requestor with a "data dump" of all digital assets held in the account.
Administrative fees.	Not addressed.	Not addressed.	A custodian may assess a reasonable administrative charge for the cost of disclosing a user's digital assets.
Deleted assets.	Not addressed.	Deleted assets need not be disclosed.	Deleted assets need not be disclosed.
Unduly burdensome requests.	Not addressed.	Court shall quash an unduly burdensome order.	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.
Fiduciary duties.	Incorporated by a generic reference to "other law."	Not addressed.	Expressly incorporated.

COMPARISON OF THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (ORIGINAL UFADAA), THE PRIVACY EXPECTATIONS AFTERLIFE AND CHOICES ACT (PEAC ACT), AND THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (REVISED UFADAA)

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Account termination.	Not addressed.	Not addressed.	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.
Joint accounts.	Not addressed.	Custodian need not disclose if aware of any lawful access to the account following the death of the user.	Custodian need not disclose if aware of any lawful access to the account after receipt of the disclosure request.
Timely compliance.	Required within [60] days, or fiduciary may request an order of compliance.	Not addressed.	Required within [60] days, or fiduciary may request an order of compliance. The order must contain a finding that disclosure does not violate 18 U.S.C. § 2702.
Custodian immunity.	Custodian is immune from liability for an act or omission done in good faith compliance with the act.	Custodian not liable for compliance in good faith with a court order issued pursuant to the act.	Custodian is immune from liability for an act or omission done in good faith compliance with the act.

Exhibit C

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:		
Microsoft Messenger:		
Yahoo! Messenger:		
ICQ:		
Google Talk:		
Jabber:		
Other:		

Financial Accounts

Intuit Quicken software password: _____

Microsoft Money software password: _____

Mint.com username & password: _____ _____

Bundle.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 SkyDrive:		
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 D

Sample language for a durable power of attorney*:

I authorize my Agent to access any digital assets[8] 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.**

---

[8] **"Digital asset" means an electronic record in which the principal 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**.

Exhibit E

Sample language for a will*:

I grant to my Personal Representative full power and authorization to deal freely with any digital assets[9] 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.**

---

[9] **"Digital asset" means an electronic record in which the principal 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.**

Exhibit F

Sample language for a trust*:

I grant to my Trustee full power and authorization to deal freely with any digital assets[10] 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.**

---

[10] **"Digital asset" means an electronic record in which the principal 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.**

Exhibit G

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.