

Is the Cloud Finally Lifting? Planning for Digital Assets

David M. Lenz, Esq.
Schneider Smeltz Spieth Bell LLP
1375 E. Ninth Street, Suite 900
Cleveland, OH 44114
(t) 216-696-4200; (f) 216-696-7303
dlenz@sssb-law.com
www.sssb-law.com

I. Data and Anecdotes About the Importance of Digital Assets

A. Recent Statistics on Digital Asset Usage: According to the Pew Internet and American Life Project:

1. The popularity of personal electronic devices has increased substantially in recent years.
 - a. Smartphone ownership in America has increased from 35% of adults in 2011 to 68% in 2015.
 - b. Tablet ownership in America has increased from 3% of adults in 2010 to 45% in 2015.
 - c. Desktop or laptop computer ownership has held steady around 72% of American adults.
2. According to a November 2016 report, 68% of American adults are on Facebook (79% of American adults who use the internet at all). Further, 62% of American seniors who use the internet are also on Facebook.

B. Digital Assets in the News: Can Survivors Access Digital Accounts? Electronic communications companies, their terms of service agreements, and federal law are all oriented toward privacy and keeping private digital information away from anyone other than the owner. This can leave fiduciaries, surviving family members, or even law enforcement, in a difficult position as they try to access information left behind.

1. **Justin Ellsworth:** This was perhaps the first significant legal fight over a deceased person's email. Justin and his father traded emails while Justin was deployed to Iraq as a Marine. They intended to complete a scrapbook after he returned. When he was killed in action in November 2004, Justin's father sought access to Justin's Yahoo! account to complete the scrapbook, but Yahoo! denied him access. After a protracted legal battle in Probate Court he was ultimately allowed to receive copies of the messages.
2. **Peggy Bush:** Peggy's husband, David, died in August of 2015. Peggy, a Canadian, had access to her late husband's iPad and knew the passcode to enter the device and enjoyed playing a particular card game on the iPad. When the game stopped working she tried to re-download it but did not know her husband's Apple ID. When she contacted Apple, they told her she would need a Court order specifically authorizing Apple to turn over the information, even though Peggy was the sole beneficiary of the

estate. Peggy went to the Court of public opinion, and after media pressure, Apple worked out its “misunderstanding” with Peggy and helped her resolve the issue.

3. Syed Farook – San Bernadino Attack: While Peggy was looking for her husband’s Apple ID, Apple and the FBI were engaged in a public legal battle about the passcode to the iPhone used by San Bernadino shooter Syed Farook. The FBI was demanding that Apple provide a work-around so it could get past the passcode screen. Apple said that it cannot run its own in-house data extraction processes on an iPhone that is running operating system iOS 8 or later. The FBI ultimately found another way to open the iPhone, but Apple’s position illustrates that not knowing the passcode can foreclose access to the contents of a smartphone.

II. “Digital Assets:” What Are We Talking About?

- A. Categories of Digital Assets: It is helpful to think of digital assets as breaking into 4 broad categories (1) electronic access to financial information, (2) purely digital assets with monetary value, (3) electronic files and resources, and (4) electronic communications. Each of these categories is discussed in more detail below.
- B. Digital Access to Financial Information: This first category is not really a “digital” asset, rather it is an electronic means to get information about other tangible or intangible assets, such as bank accounts, insurance policies, etc.

1. Examples and Significance:

- a. Logins for Bank and Brokerage Accounts. Historically, the executor of an estate may have submitted a change of address request at the post office to have the decedent’s mail forwarded to the executor’s or the attorney’s address. As paper bank statements, investment statements, and tax documents came in, the fiduciary could be sure he or she learned about most of the decedent’s assets. In a world where statements are increasingly online, relying only on paper statements may cause the executor to miss accounts. Consider whether the executor’s possible exposure for a breach of fiduciary duty if he or she fails to discover an E-Trade brokerage account that goes unmonitored and ultimately decreases in value due to a market downturn.
- b. Logins for Credit Cards and Other Online Bill Paying Accounts. Access to this information will be significant as the executor tries to learn of the decedent’s debts. Consider the case of an insolvent estate where automatic bill payments may cause the estate to pay for claims that are not entitled to priority.
- c. Logins for Home, Auto, Health, or Life Insurance. Some companies offer web-based portals that allow access to copies of the policies. If these exist, and the executor knows about them, they could be much more convenient than searching through the decedent’s file cabinets, safe, safe deposit boxes, or other storage locations to try to find current policy documents.
- d. Tax Preparation Software. The income tax return is a key document for learning about the decedent’s assets and other financial information relevant to estate administration. If the decedent filed his or her own income tax returns using TurboTax or other tax preparation software, he or she may not have a paper copy of the return. It may exist only in electronic format and, since it includes the

decedent's Social Security number, the file may be password protected to avoid identity theft.

- e. *Personal Financial Software.* If the decedent used Quicken, iBank, or any other kind of software to track his or her income and expenses, it can provide a great deal of valuable information to the executor about where the decedent's accounts are. The decedent may have even had a simple spreadsheet in Excel or other similar programs that tracked his or her investments, spending, or other financial information. Again, if this information is available to the executor it will significantly reduce the time spent looking for assets.
2. Key Question: How will the executor or guardian access this information? Will the fiduciary know that this information exists, and if so, will the fiduciary be able to access the information or will it be blocked by password access?
- C. Purely Digital Assets with Monetary Value: These assets do not have a tangible equivalent. They exist only in the digital world but may have an actual dollar value in the real world.
1. Examples:
 - a. *Web Addresses:* Buying a web address or "URL" is rather easy. One can reserve a domain through one of many providers, such as NetworkSolutions.com, GoDaddy.com, or Buydomains.com. Many can be bought and maintained for relatively small amounts (\$30 or less per year), but ultimately they can be sold for significant money—more than \$1,000,000 in some extreme cases. They are also difficult to protect in estate administration, because the annual renewal is probably tied to a credit card that will be cancelled, and the notification will go to an email address that the executor may or may not be able to access.
 - b. *Online Accounts that Hold Cash Value:* Paypal, eBay, or even an online poker account may have a stored cash value that can be recovered by an executor, though learning how to access and close these accounts may be tricky.
 - c. *Online Game Personalities:* Certain online games have mechanisms for you to sell an account to other players. A "World of Warcraft" account once sold for \$9,700. One person paid \$16,000 for a sword to be used in a video game that had not been released yet. The website www.secondlife.com allows users to buy and sell all kinds of property in a virtual world, and there are published, floating exchange rates between the currency of that virtual world ("Linden Dollars") and U.S. dollars.
 - d. *Bitcoin.* Bitcoin is a purely digital currency that allows online transfers with no "middle man." Its intended purpose is as a means of electronic exchange but it is also a volatile currency with a fluctuating exchange rate against the dollar. As of this printing, the exchange rate was \$854 to 1 Bitcoin. It's all-time high was just over \$1,100 in November 2013, and it was as low as \$203 in January 2015. Some commentators have speculated that because the supply of Bitcoin is stable and not subject to changes in monetary policy that it is becoming a new "safe" asset for a younger generation of international investors. At least one commentator has speculated that the value of 1 Bitcoin could climb to \$3,000 in 2017 due to

political and economic uncertainties in the world. Bitcoin is stored in an owner's digital "wallet" through bitcoin.org.

2. Key Questions:

- a. *How Can These Assets Be Identified and Maintained?*
- b. *Should They Be Liquidated or Distributed?* That is, would the beneficiary rather have these assets in-kind, and do the terms-of-service allow a transfer?

D. Digital Files and Resources: This is a broad category of assets that largely has more sentimental than financial value. This category represents any number of activities that are conducted electronically but may at one time have been stored in tangible form.

1. Examples:

- a. *Family Photos and Videos:* Increasingly, these items are being taken and stored in purely electronic forms. Does the decedent have a YouTube channel in which he or she stored family videos? Does the decedent use one of many cloud-based photo storage systems?
- b. *Medical Information:* Many hospital systems are giving patients online access to their own medical records. Perhaps a person wants to let his or her health care agent have access to this system to make it easier for the agent to access medical information. The American Bar Association has developed an App called "My Health Care Wishes" that allows a person to carry copies of his or her living will and health care powers of attorney in PDF form in his or her smartphone, along with other relevant personal medical information. There are also Apps for caregivers for elderly persons to help them keep track of doctor appointments, medications, and other notes relating to their daily tasks.
- c. *Organizational Information:* If a person is heavily involved in a volunteer organization, he or she may have many files that are important to that organization on his or her computer.
- d. *Sentimental Items:* One can picture any number of items from family recipes to personal notes and information relating to hobbies that may be stored electronically instead of in paper form.
- e. *Websites or blogs:* Does the client operate a website or blog? If so, is it generating advertising revenue? Could/should the contents of the blog be published as an e-book?
- f. *Planned Digital Afterlife Items:* A small industry is developing in the world of planning for one's digital afterlife. Has your client set up any of these items?
 - i. *Mywonderfullife.com:* Plan your online funeral and away messages, upload photos, and leave family members instructions about where to find your important documents and assets.
 - ii. *IfIDie App:* This app allows you to record a video or text message that will only be released on Facebook after your death is reported or confirmed by up to three "trustees."

- iii. *Digitallegacys.com*: Will create a QR Code sticker to attach to a tombstone to take users to a memorial website with photo gallery.
- iv. But beware that these sites have a tendency to develop and disappear quickly. An early competitor to Mywonderfullife.com was greatgoodbye.com, which has been offline for several years. For awhile thereafter, greatgoodbye.com would take you to a site selling skin-care products. Now there is nothing on that website. Other digital death apps that have recently gone offline include deadsoci.al (scheduled future Facebook posts after your death) and liveson.org, which allowed a computer to continue your Twitter account indefinitely.

2. Key Questions:

- a. *How Would The Executor Know These Exist Unless Told?*
- b. *Who Gets Access?* Thankfully, electronic assets are much easier to duplicate, so hopefully there is less family fighting than there might be over physical photo albums or other items of tangible personal property.

E. Electronic Communications:

1. Examples and Significance:

- a. *Email*:
 - i. *Email Accounts - You May Not Have Just One*: Note that email could be personal email accounts, work email accounts, or email accounts for social or nonprofit organizations. Family members may care about the contents of the personal email account, while other members of the organization will want to make sure they can get into an organization's email account and respond to ongoing communications.
 - ii. *Email as the Key to Digital Asset Information*: One or more email accounts are going to be the main collection point for information about a person's digital assets. If he or she is receiving electronic bank or investment statements or has any of the items described elsewhere in this outline, the information about ownership and maintenance of these digital assets will likely run through his or her email account(s). Just as U.S. Mail forwarding used to be significant for learning about assets, now access to email can be crucial.
 - iii. *Accessing Contents*: As is discussed more below, there is a significant distinction under federal computer privacy law between accessing the content of the decedent's electronic communications and accessing the decedent's record of communication. One might think of the distinction as the difference between being able to open the envelope and read each digital letter (the content) or only being allowed to see the outside of the envelope. Federal law prohibits service providers from "opening the envelope" and disclosing content of communications without authorization. This distinction under federal law makes electronic communications providers very reluctant to disclose email contents.

- iv. *Policy Considerations*: In the evolution of the law of fiduciary access to digital assets, a key policy question is how much access an executor should have to electronic communications. Should they be treated differently than tangible notes and greeting cards? The fact that most people default to saving a far greater volume of digital communication than paper communication makes electronic communication somewhat different in scale. Also, does the executor really need the content of every email to effectively administer an estate, or is it sufficient to see who the decedent was receiving emails from? For example, several emails from certain financial institutions would give the executor a strong indication that he or she should check with that institution for accounts.
- b. *Social Media*: Facebook, Twitter, LinkedIn, and Pinterest are some of the flagship items in this category, but over 200 social media sites exist for the general public or various special interests. The questions surrounding these accounts are largely oriented toward what should happen to the account, rather than how to access the contents. However, if there are concerns about the circumstances of someone's death or significant photos or other sentimental items stored in the account, access to the contents can still be a significant issue.

2. Key Questions:

- a. *What Should Happen to These Accounts?*
 - i. *Possibility for Family Disagreement*. For several years, Facebook gave family of deceased users the choice of either "memorializing" the page, to allow friends to continue to post photos, messages, and memories, or to take the page down. (In February 2015, Facebook added a much more robust "Legacy Contact" option, which is discussed more in section III(C) below.) Consider the possibility of disagreement between family members who divide into different camps based on whether they want to continue to read well-wishes from others on a memorial page or are too distraught by seeing their loved one's photo each time they open Facebook and want the profile taken down. Facebook also changed its policies in 2014 and will compile a "look back video" of photos posted by the decedent on request of a family member, after John Berlin's request for the video of his deceased son Jesse went viral.
 - ii. *Final Away Message?* In a public social media world, do your clients have final thoughts they want to share publicly, not just with family?
- b. *Who Should Have Access*: Should the executor have complete access to these accounts in all cases? What if there is some embarrassing information in an email account that the decedent would rather have deleted than accessed by family? Even if the executor is empowered to access these communications, federal law may cause the service provider to deny access.
- c. *Who Makes These Decisions?* If a client has not empowered an executor to act on these matters and arranged to give him or her access to these accounts, it may be unclear whether anyone is able to carry out the decedent's wishes.

3. New World of Digital Estate Planning: The Final Away Message: In the world of Facebook and Twitter and other social media websites, people now have a platform to communicate with multiple people simultaneously, causing them to be much more public in sharing their thoughts than they previously could be. Communication is no longer one-to-one. On social media sites, people are sharing with a wide audience everything from the humorous, to the mundane, to the profound. Do your clients want to plan a final “away message” to share spiritual truths, family philosophies, or even a last laugh?
 - a. *Andrew Olmsted*: U.S. Army Major and blogger who was killed in action on January 3, 2008. He left a message with a friend to be posted on his blog if he did not return from deployment. Check out http://obsidianwings.blogs.com/obsidian_wings/2008/01/andy-olmsted.html for a powerful reflection on life and death as a soldier and husband.
 - b. *Scott Entsminger*: Browns fan whose online obituary in the Columbus Dispatch went viral when “He respectfully requests six Cleveland Browns pall bearers so the Browns can let him down one last time.”

III. What are the Default Rules Governing Access to or Transfer of Digital Assets: Access to and transfer of digital assets at a client’s death or disability lies at the intersection of probate, contract, and intellectual property law. While our standard conceptions of probate law argue in favor of transferring these assets, contract and intellectual property law argue strongly against access and transfer.

A. Federal Law Impacts the Executor and the Communications Provider.

1. Electronic Communications Privacy Act 18 U.S.C. § 2701 et seq. (the pertinent part is also referred to as the “Stored Communications Act”).
 - a. 18 U.S.C. § 2701(a): It is a crime for anyone to intentionally access without authorization a facility through which electronic communication service is provided.
 - b. 18 U.S.C. § 2702: An electronic communication service is prohibited from disclosing communications to someone other than the originator or recipient or an agent of the originator or recipient unless they have the lawful consent of the originator or recipient. This section also distinguishes between the “contents” of a communication in 2702(b) (the actual information communicated) and “a record or other information pertaining to a” subscriber or customer in 2702(c). The contents of communications received may be disclosed only with the lawful consent of the recipient or to an agent for the recipient. The contents of communications sent may only be disclosed with the lawful consent of the sender.
2. Computer Fraud and Abuse Act 18 U.S.C. § 1030 et seq. This law prohibits accessing a computer without authorization, which has been interpreted to include not just accessing a particular machine, but accessing a computing service without proper authorization (e.g., creating a false user profile in violation of a service’s terms-of-service agreement).
3. Executor Violating Federal Law? If the executor simply takes the decedent’s passwords and starts using his or her digital assets, he or she may be in violation of

federal law. Similarly, if a service provider discloses information to an executor or family member, the *service provider* may be in violation of federal law. The concerns of service providers in this area are part of the reason for the privacy policies discussed in III.B below. Both of these problems argue for state laws to address the rights of a fiduciary as to the decedent's or ward's digital assets and for updates to the federal laws in this area. See Lamm, James, et al. "The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property." 68 U. Miami L. Rev. 385.

B. *Privacy is Key in Terms and Conditions*. Major providers of digital services want consumers to believe that their information is stored safely and kept private. Therefore, they have privacy policies that state that they will not transfer your digital information under any circumstances—even death or disability. These terms are spelled out in the so-called "clickwrap license"—the end user license agreement or "terms of service agreement" that is printed, usually in small font, above the tantalizing "I agree" button as you sign up for a new digital service. (The term "clickwrap license" derives from the term "shrinkwrap license" which refers to a license the user is deemed to have accepted by opening the shrinkwrap on a package of software purchased in a store.)¹ Below are examples of a few of the terms and conditions of major internet companies for how client accounts are handled at death.

1. GMail. (<https://support.google.com/mail/answer/14300?hl=en>) An earlier version of their policy lasted for five paragraphs, and in those five paragraphs Google stated at least three times that the decision to turn over an account-holder's content is in Google's discretion. Now the policy directs users to the "Inactive Account Manager" (discussed at III(B) below) and again states "People expect Google to keep their information safe, even in the event of their death," and "Any decision to satisfy a request about a deceased user will be made only after a careful review." The page provides an electronic form in which the executor must first provide (a) executor's name and mailing address, (b) executor's email address, (c) a photocopy of the executor's driver's license, (d) the decedent's Gmail address, (e) the death certificate. If Google determines, after initial review, that some access may be granted, it will require a U.S. Court order. However, Google will provide proposed language for the order.
2. Yahoo!. (http://help.yahoo.com/kb/index?page=content&y=PROD_GRPS&locale=en_US&id=SLN9112&impressions=true) There is no discretion in Yahoo!'s policy. The account terminates and the contents are permanently deleted. "At the time of registration, all account holders agree to the Yahoo Terms of Service (TOS). Pursuant to the TOS, neither the Yahoo account nor any of the content therein are transferable, even when the account owner is deceased."

¹ One interesting case concerning the validity of these license restrictions is *Ajemian v. Yahoo!, Inc.*, 83 Mass. App. Ct. 565 (2013). The decedent's administrator sued to obtain access to the decedent's Yahoo! Account. The Court rejected the idea that the decedent had accepted the terms and conditions—distinguishing between a "clickwrap" license where the user clicks the "I agree" button and a "browsewrap" license where the terms are available by a link but the account holder need not read or acknowledge them. *Id.* at 576. The Court remanded the case for further briefing on the issue of whether the Stored Communications Act (18 U.S.C. § 2701 et seq.) prohibited disclosure of the emails.

3. Twitter. (<https://support.twitter.com/articles/87894-contacting-twitter-about-a-deceased-user>) Twitter will simply deactivate an account upon providing the necessary documentation. “Please note: We are unable to provide account access to anyone regardless of his or her relationship to the deceased.” Twitter will also remove images or video of deceased individuals in certain circumstances. Twitter also expressly acknowledges a policy for deactivating accounts of incapacitated owners.
 4. iTunes. (<http://www.apple.com/legal/internet-services/itunes/us/terms.html#APPS>) With prior forms of music recording, it was easy enough to distribute the records or CDs a person owned to family members as tangible personal property. Now, if the music collection is amassed through iTunes, it is a violation of the terms and conditions to leave the iTunes account—or the device through which it is accessed—to the next generation. An iTunes user has “a nontransferable license to use the Licensed Application You may not transfer, redistribute, or sublicense the Licensed Application and, if you sell your Apple Device to a third party, you must remove the Licensed Application . . . before doing so.” According to these terms, when a client purchases music through iTunes, they are purchasing a personal license to listen to the music, but they are not purchasing any rights to transfer the music to the next generation.
- C. Ways to Pass Digital Information to Beneficiaries. Some of the major digital service providers are developing their own ways to allow users to manage their digital afterlife. Other third-party services purport to handle this aspect of estate planning and administration for their client across all of their digital accounts.
1. Google Inactive Account Manager. In March of 2013, Google launched its “Inactive Account Manager” which is a system that allows a user to designate a “trusted contact” to receive notification if a person’s Google account goes inactive for a specified period of time. Users may choose the length of the period of inactivity, and can choose different trusted contacts to receive notice and an opportunity to download different types of data from the Google family of services (e.g., Gmail, Google Drive, YouTube, etc.) or direct Google to delete the account without access.
 2. Facebook Legacy Contact: It is estimated there are over 30 million deceased Facebook users. In February of 2015, Facebook introduced an option allowing account holders to designate a “legacy contact” through their personal account settings.
 - a. After a death, the legacy contact is allowed to
 - i. Post information on the account holder’s behalf (e.g., a final away message or funeral information);
 - ii. Respond to friend requests
 - iii. Change profile and cover photos, and
 - iv. If the deceased account holder gives permission, download prior public posts.
 - b. The legacy contact cannot:
 - i. Log in to the deceased account holder’s account

- ii. Change past photos or posts;
 - iii. Remove friends; or
 - iv. Read the deceased owner’s messages.
3. Third-Party Beneficiary Transfers. Various websites such as Password Box (formerly Legacy Locker) allow clients to securely store their passwords and have them sent to designated beneficiaries upon a death or disability. However, be careful about giving a beneficiary access to an account with monetary value through one of these sites, as this may be considered a testamentary transfer via an electronic will that is not recognized under state law.
 4. Watch Out for Terms-of-Service Agreements. Facebook’s terms-of-service agreement prohibits sharing your password with another person, which means using a site like Password Box could be a violation of the terms of service agreement.

IV. State Law Slowly Catches Up. Not surprisingly, state law has been slow to catch up with the evolution of technology. Until 2016, only a small handful of states had laws on the books that addressed a fiduciary’s access to digital assets, and many of them did so in very limited ways. These early laws took a variety of different approaches and covered a variety of different digital assets. Around summer of 2011, the Uniform Law Commission began to explore Fiduciary Powers for Digital Assets, culminating in the Uniform Fiduciary Access to Digital Assets Act (“UFADAA”) that was approved in summer of 2014. The technology industry and privacy advocates developed a competing uniform act known as the Privacy Expectations Afterlife and Choices Act (“PEAC”) around the same time. The competition among these various approaches led to the Revised Uniform Fiduciary Access to Digital Assets Act (“RUFADAA”), which in 2016 became law in nearly half of the states, and was signed into law in Ohio on January 4, 2017. Understanding the different approaches of these various laws provides useful context for the policy choices made in RUFADAA.

- A. Pre-RUFADAA Laws Concerning Fiduciary Access to Digital Assets: The following several states were the only ones to enact legislation concerning digital assets in the era before the first Uniform Fiduciary Access to Digital Assets Act was approved in July of 2014.
 1. Connecticut and Rhode Island – Email Only: In 2005, Connecticut became the first state to address this issue with a statute that allows a fiduciary “access to or copies of the contents of the electronic mail account of such deceased person” if the executor provides (1) a written request, death certificate, and letter of authority or (2) a court order. (CONN. GEN. STAT. § 45a-334a (2015)). The statute expressly says it is not to be construed to require the service provider to violate federal law. Rhode Island followed suit in 2007 with a nearly identical law. (R.I. GEN. LAWS § 33-27-3 (2015)). These laws only deal with email accounts, which represent only a fraction of one of the four categories of electronic assets identified in this outline.
 2. Indiana – Broadens Scope of Accounts Covered: Until the Delaware law discussed below, Indiana took the broadest approach in terms of the types of assets covered of any of the states that had enacted laws concerning decedents’ digital assets. Their 2007 law requires a “custodian” to provide “access to or copies of any documents or information of the deceased person stored electronically by the custodian” if the

executor provides a written request and appropriate documentation. For those who favor fiduciary access to digital assets, the Indiana law contains two main advantages over the other states' versions. First, it applies to custodians of any kind of electronic information, so entities that store photos, videos, and other important files are subject to the law. Second, it also prohibits the custodian from destroying electronic records for two years from the date of receipt of a request. Recall that Yahoo!'s policy called for termination and deletion of an account upon notice of death. The Indiana law aims to prevent deletion before an executor can gain rightful access. (IND. CODE § 29-1-13-1.1 (2015)). The Connecticut, Indiana, and Rhode Island Laws only allowed access and copies, they did not allow control.

3. Oklahoma– Broadening from Access and Copies to Control: In 2010, Oklahoma adopted a statute that allows an executor to “take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any email service websites.” (OKL. ST. tit. 58, § 269 (2015)). This statute covered a broader range of the Electronic Communications category of digital assets, but still provided no assistance for accessing financial information, file storage, or other digital assets. It also only allowed the executor to control these items “where otherwise authorized” in compliance with federal law described above. This has been interpreted to mean only where authorized in a document (e.g., Will or power of attorney) or by Court order.
4. Idaho – No Authorization Required: Idaho Code § 15-3-715(28) (2015) is generally parallel to the Oklahoma law, but it omitted the “where otherwise authorized” language, meaning the fiduciary should have access even if not mentioned in a Will or Court order.
5. Nevada – Termination Only: In 2013 Nevada enacted a law allowing the executor to *terminate*, but *not to access*, a decedent’s electronic communications accounts. N.R.S. § 143.188 (2015).
6. Virginia – Originally Minors Only, then First to Enact New Generation: As of 2013, Virginia gave the executor of a deceased *minor’s* estate the ability to obtain the deceased minor’s electronic communications. This power did *not* extend to deceased adults. Virginia Code Ann. § 64.2-110 (2014). However, on March 26, 2015, Virginia enacted the “Privacy Expectation Afterlife and Choices Act,” which is discussed in detail in paragraph B(2) below.
7. Louisiana – Expanding on Idaho. On June 19, 2014, Louisiana enacted Code of Civil Procedure Article 3191, which gives the succession representative the authority to “take control of, handle, conduct, continue, distribute, or terminate” any digital account of the decedent. A digital account has a similar definition to the language of the Oklahoma and Idaho laws, but it also includes a “financial account Internet website, or any similar electronic services or records, together with any words, characters, codes, or contractual rights necessary to access such digital assets and any text, images, multimedia information, or other personal property stored by or through such digital account.” Thus the Louisiana law broadens at least into access to financial information, and may broaden into any type of digital asset.

8. Delaware Enacts A Broad Fiduciary Access to Digital Assets Act. On August 12, 2014, a few weeks after the Uniform Law Commission approved the Uniform Fiduciary Access to Digital Assets Act, the state of Delaware enacted its own Fiduciary Access to Digital Assets and Digital Accounts Act (Delaware Title 12, Chapter 50), based on earlier drafts of the ULC's work. It became effective at the beginning of 2015.
 - a. *Scope of Authority*. The Delaware law is the most comprehensive to be enacted, concerning all manner of "fiduciaries" including executors, guardians, agents under powers of attorney, trustees, and others. Under § 5004, "Except as otherwise provided by a governing instrument or court order, a fiduciary may exercise control over any and all rights in digital assets and digital accounts of an account holder, to the extent permitted under applicable state or federal law or regulations or any end user license agreement." The law allows a Court or an account holder to restrict access, but absent such restrictions, it is presumed that the fiduciary has full access to the digital assets or accounts.
 - b. *Effect on Service Providers and Their Reaction*. § 5005 requires custodians of electronic records to comply with fiduciary requests within 60 days and subjects the custodian to liability, including damages and attorneys' fees, if the fiduciary must bring an action and successfully forces compliance. § 5006 provides custodians immunity for good faith compliance with requests by fiduciaries under the Act. AOL, Google, and Yahoo!, among others, signed an industry letter dated July 8, 2014, urging Governor Markell to veto the Delaware law. (Available at <http://netchoice.org/wp-content/uploads/Industry-Veto-Request-of-DE-HB-345-Signed.pdf>). Their primary concerns stated in the letter are (1) that the proposed Delaware law would set default privacy settings to the lowest possible level, requiring transfer of sensitive communication to the fiduciary unless the decedent or ward makes an affirmative choice otherwise, (2) ignores contract terms in terms-of-service agreements and individuals' choices in private mechanisms such as Google's inactive account manager, and (3) traps service providers between compliance with the Delaware law and probable violation of federal law.
- B. Battle of the Uniform Law Proposals: The problem of fiduciary access to digital assets calls out for a uniform state law solution. Probate matters are generally confined to state law, but these issues impact national and multi-national companies like Apple, Google, and Facebook. If these companies are faced with a patchwork of different state laws with different authorization policies, access to different types of information, and different degrees of liability or release from liability for the service providers, they will likely continue to invoke their privacy policies to avoid sharing information.

The Delaware legislation above is not an exact match of the 2014 version of the Uniform Fiduciary Access to Digital Assets Act, but the tech industry opposition to that Act foreshadowed the conflict that would come in 2014-2015 as state legislatures struggled with whether to enact legislation on this issue and which act, if either, to choose. UFADAA and PEAC were the primary two proposed acts that competed in the state legislatures in the 2014-2015 legislative cycle. These acts provide strikingly different approaches to consumer privacy and fiduciary access.

1. UFADAA – 2014 Version. Below are a few highlights of the 2014 version of UFADAA. For a concise summary of the background of the 2014 UFADAA and the significance of its provisions, see Suzanne B. Walsh’s article “Coming Soon to a Legislature Near You: Comprehensive State Law Governing Fiduciary Access to Digital Assets,” 8 Charleston L. Rev. 429. Ms. Walsh was the Chair of the drafting committee for the Uniform Act.
 - a. *General Concepts*: The general idea of the 2014 version of UFADAA was that fiduciaries (other than guardians) generally should have access to an account holder’s information, unless he or she acts to limit that access. This includes digital assets generally, *and the content of communications*. General provisions in a terms of service agreement should not limit that access, though an account holder’s affirmative choice to limit or prohibit access should be respected.
 - b. *Access, Not Transfer*. UFADAA only governs the fiduciary’s ability to access digital assets. It does not purport to do anything about the transfer of digital assets.
 - c. *Authority of Fiduciary Over Digital Assets*. Sections 4 through 7 defined the authority of various fiduciaries over the digital assets of their decedent, ward, or principal:
 - i. **Executor**: An executor could access any digital assets including the content of electronic communications, but only if disclosing content would not violate 2702(b) of the Electronic Communications Privacy Act. However, UFADAA deemed the executor to have the lawful consent of the decedent to avoid problems under federal law. (Ideally, the Electronic Communications Privacy Act would be amended at some point to provide that disclosure to an empowered fiduciary is not a violation.) The executor’s power was broad by default but could be limited by Will.
 - ii. **Guardian**: *Only by specific order of the probate court* could a guardian or conservator access any digital assets of the ward. Again, content of electronic communications could only be granted if such disclosure would not violate 2702(b) of the Electronic Communications Privacy Act.
 - iii. **Agent**: An agent under a power of attorney had broad default powers over digital assets unless the power of attorney limited those powers. The power of attorney, however, had to specifically authorize access to the content of electronic communications.
 - iv. **Trustee**: If a Trustee was the original account holder, the Trustee had full access to the account, including content of electronic communications. If the Trustee is a successor owner of the account, a Trustee’s authority was similar to an executor’s authority.
 - d. *Broad Authority*. Sections 8 and 9 contained various provisions to help support the fiduciary’s right to access the digital assets, including provisions:
 - i. Authorizing a fiduciary to take any action the account holder could take, but recognizing that the fiduciary must act in a fiduciary capacity;

- ii. Deeming the fiduciary to have lawful consent and be an authorized user under state and federal law;
 - iii. Stating that any provision in terms-of-service agreements restricting fiduciary access is “against the strong public policy of this state,” unless it was separately agreed to by the account owner apart from the rest of the terms and conditions (that is, a person must affirmatively, specifically opt out of fiduciary access, not just include an opt-out in a clickwrap terms-of-service agreement);
 - iv. Deeming choice-of-law provisions that would restrict fiduciary access to be unenforceable;
 - v. Giving the fiduciary authority to use the decedent/ward/principal’s tangible personal property to access the electronic accounts; and
 - vi. Allowing the fiduciary to compel disclosure of the contents of communications, because under federal law disclosure would otherwise be at the custodian’s discretion.
- e. *Custodian Immunity*. Section 10 relieved custodians from liability for good faith compliance with the act.
2. Privacy Expectations and Afterlife Choices Act. The tech industry and privacy advocates had some degree of input as UFADAA was formed, but they ultimately had significant concerns with the 2014 version. NetChoice, an association of eCommerce businesses placed the 2014 version of UFADAA as number one on its 2015 Internet Advocates Watchlist For Ugly Laws (“iAWFUL”) list (<http://netchoice.org/iawful/>), and they advocated instead the adoption of the Privacy Expectations and Afterlife Choices Act (“PEAC Act,” pronounced “peace”). Among the key provisions of the PEAC Act are:
- a. *General Concept*. This act only dealt with executors. It did not address powers of attorney, guardians, or trustees. The default rule was that executors should never access content of communications unless specifically authorized by the decedent, and should be able to access other digital assets only (i) with Court authorization and (ii) if the account holder had not expressed a preference for privacy.
 - b. *Generally Access to Record of Communication Only*. Digital service providers were prohibited from disclosing contents of communication to executors unless the decedent specifically authorized it. However, an executor could file a motion supported by an affidavit with the Probate Court seeking an order to allow the executor to access the decedent’s records but *not contents of communications* for the 18-month period prior to death (or longer if special circumstances are shown). The affidavit was required to state (i) that the user is deceased, (ii) that the user was a subscriber, (iii) that the account belonging to the deceased user has been reasonably identified, (iv) there are no other authorized users of that particular account or that they have consented to the disclosure, (v) the request is tailored to effectuate the purpose of estate administration and (vi) the request is not in conflict with wishes expressed in the decedent’s Will. An order granted under this

section would give the executor access to the “outside of the envelope” only. The theory is that if the goal is to identify bank accounts or other assets, being able to see the service providers that are sending emails to the decedent will be enough to allow the executor to do his or her job without disclosing content of private communications.

- c. *Access to Content of Communication in Limited Settings.* In a similar procedure, an executor could access content of communications only if (i) the decedent expressly directed that level of access in his or her will or (ii) chose that level of access in the account settings when he or she set up the digital account.
 - d. *Service Provider Response Time.* The service providers had 60 days from receipt of an order to file a motion to quash the order for various reasons.
 - e. *Use and Control Prohibited.* Nothing in the act allowed an executor to use or control the decedent’s account.
 - f. *Executors Only.* The PEAC Act applied only to deceased account users. It provided no access for guardians or agents under powers of attorney, though the Virginia version, as enacted, directs the Joint Commission on Technology and Science to “study the implementation of this act and develop legislative recommendations to address access to electronic communication records and digital account content by guardians ad litem, conservators, and other fiduciaries.”
 - g. *Additional Discussion.* For a more thorough discussion of the argument against broad fiduciary access, see Rebecca G. Cummings’ article entitled “The Case Against Access to Decedents’ Email: Password Protection as an Exercise of the Right to Destroy Property” (15 Minn J. L. Sci. & Tech. 897 (2014)).
3. 2014-2015 UFADAA vs. PEAC Legislative Scorecard.
- a. *UFADAA:* In the 2014-2015 legislative cycle, the 2014 version of UFADAA was introduced in 27 legislatures, making it one of the most popular uniform acts ever in terms of first-year introductions. However, it was enacted in zero states.
 - b. *PEAC Act:* The PEAC Act was introduced in only a handful of states, and it was enacted in only the State of Virginia. Another solution was needed.
- C. *The Revised Uniform Fiduciary Access to Digital Assets Act or “RUFADAA”.* The apparent demand for legislation in this area, and having two proposed acts that took very opposite positions in weighing the Uniform Law Commission’s concerns in favor of access against the tech companies’ and privacy advocates’ concerns about federal law compliance and user privacy, brought both sides back to the table to try to work out a compromise uniform act. The result was a new version of UFADAA that was approved in summer 2015 by the Uniform Law Commission.
1. Legislative Success. From January of 2016 to January of 2017 it was enacted in 21 states including, most recently, Ohio.
 2. Why Did RUFADAA Gain More Support? The fundamental shift between the 2014 and the 2015 versions of UFADAA is a change from requiring users to “opt out” of fiduciary access to sensitive communication information to requiring them to specifically “opt in” to disclosure of content of communications. This preserves the

default principle of user privacy in communications (email, text messages, private messages on Facebook, etc.) while still allowing fiduciaries to get access to much of the information necessary for estate administration. Unlike the 2014 version, the 2015 version says that a fiduciary will not have access to content of communications unless the user specifically opts for that access in an estate plan document or in his or her account settings. Because many users may not be aware of this issue and may not take steps to allow fiduciary access, this will result in a default position of the custodians only being required to disclose a catalog of communications or other digital assets. The other major change is a preference toward allowing custodians to develop their own protocols for handling these issues, which will encourage the tech companies to develop systems that work for them and will have reasonable compliance costs and efficiencies. The new act also provides additional protections for custodians in dealing with requests for access. The “Enactment Kit” for the revised version of UFADAA includes endorsement letters dated October 2015 from both Google and Facebook.

D. Ohio Uniform Fiduciary Access to Digital Assets Act (O.R.C. Chapter 2137):

1. Definitions (O.R.C. § 2137.01): This section contains the definitions that apply throughout the act. A “user” is the holder of a digital asset. An “online tool” is a service separate from the terms of service agreement that allows the user to provide direction for disclosure of a digital asset to a third person. A “designated recipient” is a person entitled to receive a digital asset through an online tool. “Personal Representative” generally means an executor or administrator but also includes a commissioner under a release of assets from administration as well as an applicant for a summary release from administration. This broader definition of personal representative was included in the Ohio version of RUFADAA to avoid requiring a full estate administration to simply access sentimental digital information.
2. Scope (O.R.C. § 2137.02): Ohio’s RUFADAA will apply to all powers of attorney, guardianships, estates, and trusts, regardless of when they were established and will apply to all custodians of electronic records if the user resides in Ohio or resided here at the time of his or her death. This section also makes clear that RUFADAA does not give a fiduciary access to an employee’s business digital assets.
3. How to Decide When to Disclose (O.R.C. § 2137.03). RUFADAA sets up a new hierarchy for determining whether a fiduciary will have access.
 - a. *Use of Online Tools*. Paragraph (A) creates a preference for companies to create online tools to allow users to determine how they want their digital account to be handled. Think of an online tool as a “Transfer on Death” designation for a digital asset. An “online tool” is defined in § 2137.01(P) as an account service “distinct from the terms-of-service agreement” where a user can “provide directions for disclosure or non-disclosure of digital assets to a third person.” Examples of “online tools” include the Google Inactive Account Manager and Facebook Legacy Contact described in III(C) above. If the user has expressed a preference in an online tool, as to that digital asset, that direction “overrides a contrary direction by the user in a will, trust, power of attorney, or other record.” It is hoped that giving top priority to “online tools” will encourage more and more service providers to develop their own tools to handle these issues.

- b. *User's Direction if No Online Tools is Used or Available.* Paragraph (B) states that if no online tool is available, or it is available but not used, the user may allow or prohibit disclosure of any digital assets, *including content of communications*, by a direction in a will, trust, power of attorney, or other record.
 - c. *Terms of Service Superseded.* A direction as to account access through an online tool or in an estate planning document will supersede a contrary provision in the custodian's generic terms-of-service agreement.
4. Preservation of Terms of Service Agreement (O.R.C. § 2137.04). Paragraphs A and B state that nothing in the act changes a custodian's rights under the terms-of-service agreement, and the fiduciary does not have any new or expanded rights other than those held by the user for whom the fiduciary acts. The fiduciary's access may be limited or eliminated by (a) the user, (b) federal law, or (c) the terms of service agreement if the user did not make a specific direction concerning access recognized under § 2137.03.
5. Process for Disclosure (O.R.C. § 2137.05). When disclosing digital assets, a custodian has discretion as to whether to grant the fiduciary or recipient full access to the account, partial access to the account as needed to carry out required tasks, or copies of files the user could have accessed at the time. The custodian need not disclose digital assets deleted by the user. The custodian may also charge a reasonable fee for producing digital assets to the fiduciary. If a user directs partial disclosure that would unduly burden the custodian to segregate disclosed and non-disclosed assets, the custodian or fiduciary may petition the Court to (a) require disclosure of all assets in a specific date range; (b) require disclosure of all assets; (c) require disclosure of no assets; or (d) require disclosure of all assets for in camera review by the Court.
6. Executors: Disclosure of Content of Communications (O.R.C. § 2137.06). *If the deceased user consented to disclosure of content of communications*, the executor must provide:
- a. A written request for disclosure in physical or electronic form;
 - b. A copy of the death certificate;
 - c. A certified letter of authority or entry granting release or summary release from administration;
 - d. A copy of the Will or other document authorizing disclosure (unless disclosure was authorized using an online tool); and
 - e. As requested by the custodian, either any information identifying the user's account, or a Court order finding that (i) the user had a specific, identifiable account with the custodian, (ii) that disclosure would not violate federal law, (iii) that the user consented to the disclosure (other than through an online tool) OR (iv) that disclosure is reasonably necessary for estate administration.
7. Executors: Access to Other Digital Assets (O.R.C. § 2137.07). Because content of communications is subject to a higher privacy concern, the procedure for disclosure is somewhat more burdensome than for other digital assets. For *other digital assets*,

unless the user prohibited disclosure, or a Court directs otherwise, the custodian shall disclose a catalogue of communications sent or received, and any other digital asset (other than content of communications) in which the user had an interest if the executor provides the custodian:

- a. A written request, death certificate, or letter of authority as described in the previous section; and
- b. As requested by the custodian, any information identifying the user's account, an affidavit stating that disclosure is reasonably necessary for estate administration, or a Court order finding that (i) the user had a specific account with the custodian OR (ii) disclosure is reasonably necessary for estate administration.

Absent from this list is "a copy of the Will authorizing disclosure." That is, disclosure of these digital assets is just a part of the power of the office of personal representative. The Will need not specifically give the personal representative authority over digital assets.

8. Powers of Attorney: Disclosure of Content of Communications (O.R.C. § 2137.08). If a power of attorney *expressly grants authority over the content of communication*, the custodian must disclose content of communications if the custodian is presented with (a) a request for the information, (b) a copy of the power of attorney, (c) a certification by the agent under penalty of perjury that the power of attorney remains in effect, and (d) as requested by the custodian, information to identify the principal's account. If the power of attorney does not specifically give access to content of communications, no disclosure of content of communications is required.
9. Powers of Attorney: Access to Other Digital Assets (O.R.C. § 2137.09). *Any digital assets other than content of communication* must be disclosed to the agent under a general power of attorney when he or she provides the same information described in the previous section. A general power of attorney does not need to specifically mention access to digital assets to have the effect of allowing access to digital assets other than content of communications.
 - a. *Limiting Agent Access*. The agent's authority to access digital assets may be limited by (i) a court order, (ii) language in the power of attorney limiting such access, or (iii) separate instructions by the principal directing that the agent should not have access.
 - b. *Change to Statutory Form Power of Attorney*. House Bill 432, which enacted RUFADAA also modified the statutory form power of attorney under O.R.C. § 1337.60. "Digital assets" are now included as a category of assets for which a principal may initial the corresponding line on the form to give authority to his or her agent. In addition, there is a separate line for the principal to initial to give the agent authority to access content of communications.
10. Trustees as Original Account Users (O.R.C. § 2137.10). This section makes clear that if the Trustee is the original user of the digital assets, the Trustee may access any of those assets, including content of communication, unless otherwise ordered by the Court.

11. Trustees who are not Original Account Users – Disclosure of Content of Communications (O.R.C. § 2137.11). If the Trustee is not the original account user, the rules governing Trustees are substantially the same as the rules governing executors, and content of communications must be disclosed if the Trustee provides:
 - a. A written request for disclosure in physical or electronic form;
 - b. A copy the Trust instrument showing authority to receive content of communications and a statement under penalty of perjury that the Trustee is the currently acting Trustee OR a certification of Trust under O.R.C. § 5810.13 that includes a statement that the Trustee is authorized under the Trust to receive content of communication;
 - c. As requested by the custodian, either any information identifying the trust’s account, or evidence linking the account to the trust. (Note that this section does not reference Court orders of a similar type to those described under item 6(e) above pertaining to executors.)
12. Trustees who are not Original Account Users – Access to Other Digital Assets (O.R.C. § 2137.12). Unless otherwise limited by the Trust instrument or court order, any digital assets other than content of communication must be disclosed to the Trustee when they provide the custodian the same information described in the previous section—except that the Trustee’s certification is limited to certifying that he or she is the Trustee, not that he or she has any specific powers over digital assets
13. Guardians (O.R.C. § 2137.13). Access to digital assets is *not* an inherent part of the office of Guardian.
 - a. *Hearing Required*. Paragraph A states that guardians will have access if the Court grants access after an opportunity for a hearing. A Guardian will get access to assets *other than content of communication* when the Guardian provides the custodian
 - i. A written request for disclosure
 - ii. A copy of the court order that gives the guardian authority to access digital assets; and
 - iii. As requested by the custodian, either any information identifying the ward’s account, or evidence linking the account to the ward.
 - b. *No Access to Content of Communication*. There is no provision for a Guardian to access the content of a ward’s communication. Presumably this is because appointment of a guardian is an involuntary process and there is a higher interest in preserving the ward’s right to privacy.
 - c. *Termination of Accounts*. Paragraph C states that the Guardian may, without court order, request a custodian terminate an account of the ward for good cause. Such a request must be accompanied by the Guardian’s general letters of authority. This provision is designed to allow the Guardian to terminate an account if there are identity theft issues or if the ward is using the account for inappropriate activities.

14. Other Fiduciary Duties and Authority (O.R.C. § 2137.14). In dealing with digital assets fiduciary still must act in accordance with its duties of care, loyalty, and confidentiality. The fiduciary is subject to other laws, including the terms-of-service agreements, in dealing with digital assets except as provided in § 2137.03 (where an account user may give a fiduciary broader access than provided in the terms of service agreements). The fiduciary may not use the account to impersonate the user.
- a. *Access to Other Digital Assets*. Paragraph C states that RUFADAA is not limited to access to assets stored with a custodian. The fiduciary's authority extends to other digital assets not subject to a custodian or a terms of service agreement (e.g., files generated by the user and stored on his or her home computer).
 - b. *Access to Tangible Personal Property*. Paragraphs D and E make clear that the fiduciary acting within the scope of his or her duties is authorized to use and access the user's computers, smartphones, or other tangible personal property to access his or her digital assets for purposes of any applicable computer fraud laws, including O.R.C. § 2913.04.
 - c. *Terminating Accounts*. Sections 2137.06 through 2137.13 are designed to govern different types of fiduciaries' access to the user's accounts. Paragraphs F and G of § 2137.14 provide authority for any type of fiduciary to terminate a user's account. To terminate, the fiduciary must only provide a copy of the same types of documents described in the preceding sections showing that he or she has general authority over digital assets described above.
15. Custodian Compliance (O.R.C. § 2137.15). Custodians generally must comply with requests for access within 60 days, and a fiduciary or designated recipient may seek a Court order requiring compliance if it is not timely. The custodian may attempt to notify the user if it receives a request for access under RUFADAA, and it may deny a request if it believes the user has lawfully accessed the asset after the request is received. Custodians may obtain or require an Agent, Guardian, or designated recipient to obtain a Court order finding that the account belongs to the user, that there is sufficient consent from the ward or principal to support the disclosure, and disclosure will not otherwise violate state or federal law. As with the 2014 version, custodians remain immune from liability for good faith compliance with the Act.
16. Uniform Interpretation (O.R.C. § 2137.16). Courts are specifically requested to consider the need to promote uniformity of the law among states when interpreting the provisions of RUFADAA.

V. What Can Individuals Do to Plan for Digital Assets? The enactment of RUFADAA in Ohio provides fiduciaries much greater standing to access and deal with users' digital assets than they have had historically, and it allows fiduciaries to access most digital assets without specific authorization in the user's estate plan. However, RUFADAA does not eliminate the need to plan for digital assets:

- A. *Create a Digital Inventory*. This is the single most important step in allowing a client's digital estate to be properly administered. Without some kind of listing of important digital assets, the executor will be powerless to know if any digital assets exist or where they are.

1. *List Usernames and Passwords.* Despite the warnings of every internet security article you have ever read, it can be very beneficial to have a list of usernames and passwords that the fiduciary can access. Such a list should, obviously, be stored in a secure location. Consider storing it on a flash drive, which is in turn placed in a secure location or consider using various internet applications that serve as password vaults (e.g., Keeper, LastPass, or 1Password).
 2. *List where to find important files.* If there are financial files, photos, videos, or other information that will be important to survivors, list where these items are stored.
- B. *Express Wishes for What Should Happen to Digital Assets.* If there are accounts a user wants deleted, or if he or she wants to post a final “away message,” these goals should be written down, or they should use one of the online services that will arrange such messages.
- C. *Watch for Online Tools.* As RUFADAA is enacted in more and more jurisdictions, more and more custodians will be developing online tools to deal with account access after death. Take advantage of these tools as the easiest way to provide an orderly transition of digital assets. However, remember that as with other beneficiary designations, it will be important to keep these up to date. For example, there is no provision in the law automatically revoking an online tool designation in favor of an ex-spouse in the event of a divorce after the tool is set up!
- D. *Think About Physical Assets to Access Digital Information:* Whatever a person’s digital presence is, they are bound to have various electronic devices that allow them to access their digital world. Giving the fiduciary the ability to access that information will enhance the chance that all relevant digital assets will be preserved.
1. Home Personal Computer: Historically this would be the first stop for a search of a decedent’s digital presence. It might show whether he or she was using tax preparation or financial management software, or it might have certain passwords to online accounts auto-saved into the web browser that would allow an executor, a guardian, or a power of attorney access. Key questions to consider with the home computer include:
 - a. Do you need a password to log on to the computer at start-up?
 - b. Are important files organized into folders or otherwise easily found?
 - c. Does the executor have an obligation to search the home computer for information the family may find valuable for sentimental purposes?
 2. Cloud-Based Storage: Dropbox, iCloud, OneDrive, and Google Drive are among the many cloud-based storage systems that allow a person to access files from any device. Did the decedent have one or more accounts, and does the executor know the password?
 3. External Hard Drives, Flash Drives, and Memory Cards: Do these other storage devices contain photos or other files? Are they organized and labeled? Can they be found and searched?
 4. Tablets and Smartphones: Photos are increasingly being taken by smartphones and tablets. Also, as tablets slowly start to replace home PCs in terms of their importance

in a client's computing life, the executor may want to investigate what apps the decedent was using and what information is stored there.

VI. How Can We Help Our Clients in the Meantime?

A. Update our Documents.

1. **Give Explicit Digital Asset Powers and Consider Access to Content of Communication.** We should be including digital asset powers in our powers of attorney and wills. Despite the enactment of RUFADAA and its specific provisions for Trustee access, I favor placing a digital asset power in a will over a trust, because you can provide the digital service provider letters of authority showing that you are the fiduciary without needing to take the extra step of showing how the digital assets were transferred into the trust. Remember that attempted transfer of digital assets can be a violation of some terms of service agreements. In adding this language, note the "authorized user" and "lawful consent" issues in federal law. *In drafting documents under RUFADAA, the decision point for clients will be whether they want the executor or the power of attorney to have access to content of communications.* If so, they will need to state that explicitly. Remember, Ohio's enactment of RUFADAA changed the statutory form Power of Attorney for that purpose, so clients will need to update these documents if they want to grant access to content of communications.
2. **Give Robust Delegation Powers.** The client may want to designate a particularly tech-savvy family member to serve as a "digital executor" (e.g., an adult child instead of a surviving spouse). If so, the Will should have a solid delegation power that will allow the "digital executor" to work directly with service providers.

- B. **Consider a Digital Property Memorandum.** Many clients prepare "tangible personal property memoranda" to dispose of personal effects. Digital assets are natural for being dealt with in an informal memorandum, since they are constantly changing and it may be inappropriate to put certain aspects of digital information directly in the client's will.