ESTATE PLANNING IN THE DIGITAL AGE

Sponsor: Young Lawyers Division
CLE Credit: 1.0
Thursday, June 19, 2014
9:40 p.m. - 10:40 a.m.
Ballroom C
Northern Kentucky Convention Center
Covington, Kentucky

A NOTE CONCERNING THE PROGRAM MATERIALS

The materials included in this Kentucky Bar Association Continuing Legal Education handbook are intended to provide current and accurate information about the subject matter covered. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of this Kentucky Bar Association CLE program disclaim liability therefore. Attorneys using these materials, or information otherwise conveyed during the program, in dealing with a specific legal matter have a duty to research original and current sources of authority.

Printed by: Evolution Creative Solutions
7107 Shona Drive
Cincinnati, Ohio 45237

Kentucky Bar Association

TABLE OF CONTENTS

THE PRESENTERS

Heather Pack Howell
Fogle Keller Purdy PLLC
300 East Main Street, Suite 400
Lexington, Kentucky 40507
(859) 253-4700
hhowell@fkplaw.com

HEATHER PACK HOWELL is an attorney with Fogle Keller Purdy PLLC in Lexington, where she leads the firm's growing estate practice. Ms. Howell received her B.A., *magna cum laude*, from the University of Kentucky and her J.D. from the University of Kentucky College of Law. She is admitted to practice before the United States District Court for the Eastern District of Kentucky and is a member of the Fayette County and Kentucky Bar Associations.

D. Lyle McQuinn
Goeing, Goeing and McQuinn PLLC
2312 Lilac Park
Lexington, Kentucky 40509
(859) 744-4004
lmcquinn@kylawpractice.com

D. LYLE MCQUINN is an attorney with Goeing, Goeing and McQuinn PLLC in Lexington, where he focuses his practice in the areas of trusts and estates, probate, special needs trusts, Medicaid planning and charitable planning. Mr. McQuinn is the Chair of the firm's Trusts and Estates practice group. He is a graduate of Eastern Kentucky University and received his J.D. from the University of Kentucky College of Law and his L.L.M. from the University of Florida College of Law. Mr. McQuinn is a member of the Fayette County and Kentucky Bar Associations and the Bluegrass Estate Planning Council.

I. WHAT ARE DIGITAL ASSETS?

A. In General

A digital asset is any information about you or created by you that exists in digital form, either online or on an electronic storage device, including the information necessary to access the digital asset.[1]

B. Four Types of Digital Assets

There are four categories of digital assets: personal, financial, business and social media.[2]

1. Personal: files stored on a computer, smartphone or onto a website.

2. Financial: bank accounts, Amazon accounts, PayPal accounts, accounts with other shopping sites or online bill payment systems.

3. Business: customer addresses and patient or client information.

4. Social media: assets that generally entail social interactions with a network of people through websites, such as Facebook and Twitter, and email accounts.

II. ISSUES THAT ARISE AT DEATH?

A. The Importance of Locating Digital Assets

1. Gathering assets.

Personal representatives have a duty to gather the assets of the estate. However, this process has been complicated with the introduction of online accounts. Presently, many clients have financial accounts with paperless statements. In days gone by, attorneys advised personal representatives to go through the decedents' mail and personal papers to find account statements. While this continues to be good advice, many clients now have

[1] A Helpful Overview of All Your Digital Property and Digital Assets, Everplans, https://www.everplans.com/articles/a-helpful-overview-of-all-your-digital-property-and-digital-assets, (last updated May 5, 2014).

[2] Marie Perrone, "What Happens When We Die: Estate Planning of Digital Assets," 21 CommLaw Conspectus 185 (2012-2013).

financial accounts that are handled exclusively online. If there are no paper statements or lists of accounts with account numbers, the Executor or Administrator can have a difficult time locating these assets. A personal representative who fails to investigate the presence of online accounts is in violation of his or her duty as a fiduciary.

2. Paying debts.

Yet another duty of the personal representative is the payment of decedent's debts. While some billing comes in paper format to the decedent's home, many clients are now enrolled in paperless billing. Without access to the decedent's email account(s), knowing what bills need to be paid can be a difficult process for the personal representative.

3. Securing the estate.

Fiduciaries have an obligation to secure the estate by cancelling credit cards and closing accounts. This is an important step to take to prevent fraud against the estate. Without appropriate information regarding digital accounts, this can be problematic.

B. Problems Gaining Access to Digital Accounts and Assets

1. Website service agreements.

When a user registers a new account on a website, social media page, or email service provider, he or she is required to sign a website service agreement, also termed a terms of service agreement (TSO). Most TSOs state that the account is "not transferrable." While I would argue that allowing an Executor or Administrator access to the account does not a "transfer," many service providers rely on this language to deny personal representatives access to the accounts.

a. Social media.

Gaining access to the decedent's social media accounts such as Facebook, Twitter, Instagram, and the like can be difficult, if not impossible, without appropriate login information. Unfortunately, most social media companies are reluctant to allow personal representatives access to the accounts.

i. Facebook.

According to Facebook's stated policy, citing privacy concerns, it will not provide login information

to a deceased person's account. It does provide two options:

a) Memorializing the account.

Basically changes the page to a memorial page and allows only "Friends" to search for the page.

b) Removal of the account.

c) Steps.

The person requesting memorialization or removal must prove his/her relationship to the decedent and provide appropriate documentation, such as a death certificate, birth certificate or order of appointment of personal representative.[3]

ii. Twitter.

Like Facebook, Twitter does not allow access to decedent's account; however, a personal representative or immediate family member can request that the account be deactivated. To request deactivation, the following information must be provided:

a) The username of the deceased user's Twitter account (*e.g.*, @username or twitter.com/username);

b) A copy of the deceased user's death certificate;

c) A copy of the requesting party's government-issued I.D. (*e.g.*, driver's license);

d) A signed statement including: the first and last name, email address and contact information of the requesting party;

e) The relationship to the deceased user or their estate;

[3] "Special Request for Deceased Person's Account," Facebook, http://www.facebook.com/help/contact/228813257197480, (last updated May 5, 2014).

f) The action requested (*e.g.*, 'please deactivate the Twitter account');

g) A brief description of the details that evidence this account belongs to the deceased, if the name on the account does not match the name on the death certificate; a link to an online obituary or a copy of the obituary from a local newspaper (optional).[4]

iii. Instagram.

As Instagram is owned by Facebook, their policies are very similar. Instagram will not allow access to a deceased person's account, but will remove the account upon request with some basic information and a copy of the death certificate.[5]

iv. LinkedIn.

Though it does not contain as much personal information about the deceased person as Facebook, Instagram or Twitter, the decedent's profile on LinkedIn should be addressed. LinkedIn allows for the removal of the page with a few simple steps.[6]

b. Email accounts.

Perhaps the most important accounts necessary for personal representatives to access are the decedent's email accounts. Email can be the key to discovering assets and debts belonging to the decedent. Unlike social media, which almost universally denies the personal representative or family member access to the account, there is much more variance in the treatment of email accounts.

i. Google.

Google's policy regarding its Gmail accounts is that it may, under rare circumstances, provide access to the decedent's account. The determination is made

[4] "Contacting Twitter about a Deceased User," Twitter, https://support.twitter.com/articles/87894-contacting-twitter-about-a-deceased-user# (last updated May 5, 2014).

[5] "Report a Deceased Person's Account on Instagram," Instagram, https://help.instagram.com/contact/396019703850735, (last updated May 5, 2014).

[6] "Deceased LinkedIn Member-Removing Profile," LinkedIn, http://help.linkedin.com/app/answers/detail/a_id/2842/~/deceased-linkedin-member---removing-profile (last updated May 5, 2014).

after a two-step process, which may take months to complete. The first step involves collecting some basic information, including a death certificate and a copy of an email that the requesting party received from this email address. If you make it beyond step one, step two requires additional information, including a court order. Google makes abundantly clear that they may or may not allow access to the account, even if all of the requested information is provided. Detailed instructions are available on their website.[7]

ii. Yahoo.

Citing the user agreement that is signed at the time an account is opened, Yahoo states that accounts are not transferable. As such, Yahoo does not allow access to the account information of a deceased person. They will honor a request to close the account upon the receipt of the following information:

a) A letter containing your request and stating the Yahoo ID of the deceased.

b) A copy of a document appointing the requesting party as the personal representative or executor of the estate of the deceased.

c) A copy of the death certificate of the Yahoo account holder.[8]

iii. Outlook.com.

Microsoft has a Next of Kin process for Outlook.com accounts, *i.e.* accounts ending in @outlook.com, @hotmail.com, @live.com, @windowslive.com, or @msn.com. The Microsoft Next of Kin process allows for the release of Outlook.com contents, including all emails and their attachments, address book, and Messenger contact list, to the next of kin of a deceased or incapacitated account holder and/or closure of the

[7] "Accessing a Deceased Person's Email," Google, https://support.google.com/mail/answer/14300?hl=en, (last updated May 5, 2014).

[8] "Options Available When a Yahoo Account Holder Passes Away," Yahoo, https://help.yahoo.com/kb/SLN9112.html?impressions=true, (last updated May 5, 2014).

Microsoft account, following a short authentication process. They cannot provide you with the password to the account or change the password on the account, and cannot transfer ownership of the account to the next of kin. Account contents are released by way of a data DVD which is shipped to the requesting party.[9]

2. Privacy laws.

In addition to running up against website service agreements, when conducting their search for digital assets, personal representatives also must consider state and federal privacy laws.

a. Stored Communications Act.

As part of the Federal Electronic Communications Privacy Act, Congress enacted the Stored Communications Act.[10] The SCA provides that any "person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[11] Providers often cite this law, in addition to their own website service agreements, in denying access to decedents' accounts.

b. Computer Fraud and Abuse Acts.

In addition to the Stored Communications Act, there are also Federal and State Computer Fraud and Abuse Acts. 18 U.S.C. §1030(a)(2)(c) says, "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication;…. shall be punished as provided in subsection (c) of this section. Personal representatives, would likely fall under the category of "authorized users" as far as decedents hard drive is concerned. But, accessing online accounts is different because those accounts are also subject to terms of service agreements. "The problem is that (some would say) overzealous prosecutors are using the CFAA to

[9] "My Family Member Recently Died / Is In A Coma What Do I Need to Do to Access Their Microsoft Account?" Microsoft, http://answers.microsoft.com/en-us/outlook_com/forum/oaccount-omyinfo/my-family-member-died-recently-is-in-coma-what-do/308cedce-5444-4185-82e8-0623ecc1d3d6 (last updated May 5, 2014).

[10] 18 U.S.C. §§2701-2711.

[11] 18 U.S.C. §2702(a)(1).

prosecute defendants based solely on violations of a website's TOSA. The Aaron Swartz case was the most recent, highly publicized example of such a prosecution. Aaron Swartz was a self-described internet activist who committed suicide in 2013, while facing prosecution for downloading, without permission, 4.8 million academic articles from the JSTOR digital library system (http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide)."[12]

c. State privacy laws.

In addition to the federal privacy laws discussed above, each state has its own set of regulations that govern computer related crimes. The Natural Conference of State Legislatures provides the following quick guide to state law.[13]

STATE	CITE
Alabama	Ala. Code §§13A-8-112, 13A-8-113
Alaska	Alaska Stat. §11.46.740
Arizona	Ariz. Rev. Stat. §§13-2316 to 13-2316.02
Arkansas	Ark. Code §§5-41-101 to -206
California	Cal. Penal Code §502
Colorado	Colo. Rev. Stat. §18-5.5-101 to -102
Connecticut	Conn. Gen. Stat. §53a-250 to 53a-261
Delaware	Del. Code tit. 11, §931 to 941
Florida	Fla. Stat. §815.01 to 815.07
Georgia	Ga. Code §§16-9-90 to 16-9-94, §§ 16-9-150 to 16-9-157
Hawaii	Hawaii Rev. Stat. §§708-890 to 708-895.7
Idaho	Idaho Code §18-2201, §18-2202
Illinois	720 ILCS §5/17-50 to -55
Indiana	Ind. Code §§35-43-1-4, 35-43-2-3
Iowa	Iowa Code §716.6B
Kansas	Kan. Stat. Ann. §21-5839
Kentucky	Ky. Rev. Stat. §§434.840, 434.845, 434.850, 434.851, 434.853, 434.855, 434.860
Louisiana	La. Rev. Stat. Ann. §§14:73.1 to 14:73.8
Maine	Me. Rev. Stat. Ann. tit. 17-A, §431 to 435
Maryland	Md. Code, Crim. Law §7-302
Massachusetts	Mass. Gen. Laws Ann. ch. 266, §33A

[12] Suzanne Brown Walsh, "Digital Death: Dealing With Digital Property of the Estate," 40th Annual Midewest/Midsouth Estate Planning Institute (July 2013).

[13] "Computer Crime Statutes," Natural Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (last updated, May 5, 2014).

Michigan	Mich. Comp. Laws §§752.791, 752.792, 752.793, 752.794, 752.795, 752.796, 752.797
Minnesota	Minn. Stat. §§609.87 to 609.893
Mississippi	Miss. Code §97-45-1 to 97-45-33
Missouri	Mo. Rev. Stat. §537.525, § 569.095, §569.097, §569.099
Montana	Mont. Code Ann. §45-2-101, § 45-6-310, § 45-6-311
Nebraska	Neb. Rev. Stat. §§28-1341 to 28-1348
Nevada	Nev. Rev. Stat. §205.473 to 205.513
New Hampshire	N.H. Rev. Stat. Ann. §§638:16, 638:17, 638:18, 638:19
New Jersey	N.J. Rev. Stat. §§2A:38A-1 to -3, § 2C:20-2, §§ 2C:20-23 to 34
New Mexico	N.M. Stat. Ann. §30-45-1 to 30-45-7
New York	N.Y. Penal Law §156.00 to 156.50
North Carolina	N.C. Gen. Stat. §14-453 to 14-458
North Dakota	N.D. Cent. Code §12.1-06.1-08
Ohio	Ohio Rev. Code §§2909.01, 2909.04, 2909.07(A)(6), 2913.01 to 2913.04
Oklahoma	Okla. Stat. tit. 21, §§1951 to 1959
Oregon	Or. Rev. Stat. §164.377
Pennsylvania	18 Pa. Stat. §5741 to 5749
Rhode Island	R.I. Gen. Laws §11-52-1 to 11-52-8
South Carolina	S.C. Code §16-16-10 to 16-16-40
South Dakota	S.D. Cod. Laws §43-43B-1 to §43-43B-8
Tennessee	Tenn. Code §§39-14-601 to -605
Texas	Tex. Penal Code §33.02
Utah	Utah Code §76-6-702 to 76-6-705
Vermont	Vt. Stat. Ann. tit. 13, §4101 to 4107
Virginia	Va. Code §§18.2-152.1 to -152.15, § 19.2-249.2
Washington	Wash. Rev. Code §9A.52.110, §9A.52.120, §9A.52.130
West Virginia	W. Va. Code §§61-3C-3 to 61-3C-21
Wisconsin	Wis. Stat. §943.70
Wyoming	Wyo. Stat. §6-3-501 to §6-3-505

3. What does Kentucky say?

Our regulations are set forth in KRS §§434.840, 434.845, 434.850, 434.851, 434.853, 434.855, 434.860.

a. KRS 434.845 "Unlawful access to a computer in the first degree"

> (1) A person is guilty of unlawful access to a computer in the first degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of:

(a) Devising or executing any scheme or artifice to defraud; or

(b) Obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises.

(2) Unlawful access to a computer in the first degree is a Class C felony.

b. KRS 434.850 "Unlawful access to a computer in the second degree"

(1) A person is guilty of unlawful access to a computer in the second degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, which results in the loss or damage of three hundred dollars ($300) or more.

(2) Unlawful access to a computer in the second degree is a Class D felony.

c. KRS 434.851 "Unlawful access in the third degree"

(1) A person is guilty of unlawful access in the third degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, which results in the loss or damage of less than three hundred dollars ($300).

(2) Unlawful access to a computer in the third degree is a Class A misdemeanor.

d. KRS 434.853 "Unlawful access in the fourth degree"

(1) A person is guilty of unlawful access in the fourth degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly

accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, which does not result in loss or damage.

(2) Unlawful access to a computer in the fourth degree is a Class B misdemeanor.

e. KRS 434.855 "Misuse of computer information"

(1) A person is guilty of misuse of computer information when he or she:

(a) Receives, conceals, or uses, or aids another in doing so, any proceeds of a violation of KRS 434.845; or

(b) Receives, conceals, or uses or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing the same to have been used in or obtained from a violation of KRS 434.845.

(2) Misuse of computer information is a Class C felony.

f. What does all of that mean for personal representatives?

Given the language of the statute, it seems unlikely that a personal representative would run afoul of Kentucky's privacy laws. Just to be safe, I would recommend to the personal representative that he or she should wait until the court has issued the order of appointment, so that he or she has authority to act on behalf of the estate. I think this would amount to "effective consent" under the statute and would therefore prevent any issue under the Kentucky statutes. That still does not mean that the personal representative isn't violating a TOSA, unless he or she is following the protocol of that particular company.

4. States that have addressed the need for access to digital assets.

Numerous states have adopted their own statutes to govern the fiduciary's access to digital assets. To date, Connecticut, Rhode Island, Indiana, Oklahoma, and Idaho have each adopted

statutory schemes to deal with access to digital information.[14] Some states, such as Connecticut and Rhode Island, enacted statutes that apply only to email accounts.[15] Indiana's statute applies to "electronically stored documents or information."[16] Oklahoma and Idaho have states that apply to "social networking, microblogging/SMS, and e-mail accounts."[17] Kentucky currently has no legislation in this area. Websites such as "Everplans" provide a good running tally of which states have laws and what those laws entail.[18]

5. Uniform Law Commission.

The Uniform Law Commission has a Committee titled "Fiduciary Access to Digital Accounts." The Committee includes representatives of many major players including Facebook, Google and Microsoft. Their role is to "draft a free-standing act and/or amendments to ULC acts, such as the Uniform Probate Code, the Uniform Trust Code, the Uniform Guardianship and Protective Proceedings Act, and the Uniform Power of Attorney Act, that will vest fiduciaries with at least the authority to manage and distribute digital assets, copy or delete digital assets, and access digital assets."[19] A draft of the proposal is available for review on the ULC's website. "March 21st marks the last formal meeting of the committee, as the drafting process is coming to a close and the act is likely scheduled for approval by the ULC in the summer."[20]

[14] "Estate Laws Regarding Digital Assets," the digital beyond, http://www.thedigitalbeyond.com/law/, (last updated May 5, 2014).

[15] Conn. Gen. Stat. §45A-334A(2012); R.I. Gen. Laws Ch. 33-27 (2012).

[16] Ind Code §29-1-13-1.1 (2012).

[17] Okla. Stat. Tit. 58 §269 (2012).

[18] "State-By-State Digital Estate Planning Laws," Everplans, https://www.everplans.com/tools-and-resources/state-by-state-digital-estate-planning-laws, (last updated May 5, 2014).

[19] "Fiduciary Access to Digital Accounts," Uniform Law Commission, http://www.uniformlaws.org/Committee.aspx?title=Fiduciary+Access+to+Digital+Assets. (last updated May 5, 2014).

[20] Evan Carroll, "ULC Fiduciary Access to Digital Assets Committee Work Coming to Close," the digital beyond, http://www.thedigitalbeyond.com/2014/03/ulc-fiduciary-access-to-digital-assets-committee-work-coming-to-close/, (last updated May 5, 2014).

III. PLANNING TECHNIQUES

A. Ask Your Clients

Whether you are drafting a simple will or a complicated estate plan, digital assets must be discussed with your clients along with their traditional assets. Most clients probably do not think of email accounts or social media pages as "assets." We must counsel them on the potential pitfalls of not addressing digital assets and help them plan so that many of these problems can be avoided.

B. Planning Tools

1. Inventory.

Have the client create an inventory of online accounts including usernames and passwords. Due to the fact that passwords are constantly changing, the list should be somewhat accessible by the client. However, it should be secure as the loss of this information can be financially devastating. In addition, there are several online programs available that can help clients keep track of passwords. They are password management programs that allow the user to save all password information in one place and require only one password to gain access to all of the client's passwords.

a. KeePass Password Safe: http://keepass.info/.

b. 1 Password: https://agilebits.com/onepassword.

2. Simplify accounts.

There are things your clients can do to make the process a bit easier for the personal representative. First, advise your clients to consolidate accounts. They shouldn't have CDs at twenty different banks. Nor should they have ten different email addresses. Unless there is a real need for so many accounts, advise them to whittle their email accounts to a manageable number and consolidate assets into fewer institutions.

3. Keep some paper records.

Although we are all trying to cut down on paper, for environmental and practical reasons, having some paper documentation regarding one's assets is advisable. I advise clients to keep a binder to house all important financial information. Just one copy of a of bank statement, credit card statement, investment account, etc. can go a long way toward making life easier for the personal representative. Again, this information should be secure to avoid the unnecessary risk of it falling into the wrong hands.

4. Store documents on the cloud.

   Clients can store passwords, account information, even their estate planning documents, themselves, on a cloud based storage system. For those unfamiliar with cloud storage, it is defined as "a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers and multiple locations. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage."[21]

5. Social media.

   Some social media sites allow clients to make advance arrangements for their social media accounts.

   a. Google has an "Inactive Account Manager" that allows clients to share their accounts at death by choosing a period of inactivity after which to contact a "trusted contact." Once the specified period of time has lapsed, Google sends an email to the trusted contact advising that the account has been inactive for a period of time. It also specifies the level of access the Google user granted to the trusted contact at the time the account was set up. Google gives the trusted contact a certain period of time in which to download the shared data. A verification process takes place before the data is shared. Given Google's rather stringent process to gain access to accounts after death, it is advisable that clients take advantage of this option if they want to share this information at death.[22]

   b. Facebook has an app titled "If I Die." It allows users to create a message or video to be posted to Facebook in the event of death.[23]

---

[21] "Cloud Storage," Wikipedia, http://en.wikipedia.org/wiki/Cloud_storage (last updated May 5, 2014).

[22] "Inactive Account Manager for Trusted Contacts," Google, https://support.google.com/accounts/answer/3036514 (last updated May 5, 2014).

[23] "What Happens to Your Facebook Profile if You Die," Facebook, http://www.ifidie.net/ (last updated May 5, 2014).

IV. WHAT IF THE DECEDENT DID NOT HAVE A DIGITAL ESTATE PLAN?

Assume that you are contacted by a personal representative to probate an estate and the decedent had no plan in place to address his or her digital assets. Now what?

A. Order a copy of the client's credit report. This may give some insight into what debts are outstanding.

B. Check bank statements, if available. If not, and you know where the client banked, you can order copies of old statements. Bank statements are helpful in determining what monthly bills decedent was incurring at the time of his or her death, what bills are on automatic withdrawal, any payments to insurance companies (which may provide information about life insurance policies), etc. Reviewing the deposits can give the personal representative valuable information regarding deposits from annuities, dividends and the like.

C. Check the decedent's tax returns for the years leading up to death. They will provide helpful information regarding income received from decedent's investments.

D. Check the history on the decedent's computer or smart phone to see what websites he or she visited. Of course, be mindful of the privacy laws previously discussed.

E. Attempt to gain access to email accounts. It is advisable to follow the steps provided by the service provider to make sure that you aren't running afoul of the TOSA.

V. CONCLUSION

Digital assets are here to stay, at least for the foreseeable future. In order to adequately represent our clients, we must start addressing them in our estate planning documents and when representing fiduciaries in the administration of estate. While Kentucky has not yet implemented a set of laws dealing with the treatment of digital assets, we should make our clients aware of the necessity of planning ahead so that their personal representatives are made aware of what accounts are in existence and how they may access them.