SPIDERS FROM MARS: UPOAA, UFADAA & ZIGGY STARDUST

By Richard E. Davis, Esq.

Krugliak, Wilkins, Griffiths & Dougherty Co., L.P.A.
Canton, Ohio
Member, PLJO Editorial Advisory Board
and

Matthew R. Hochstetler, Esq.

Day Ketterer Ltd.
Canton, Ohio

One can hardly study the subject of the Uniform Power of Attorney Act ("UPOAA") and the Uniform Fiduciary Access to Digital Assets Act ("UFADAA") without becoming aware of the uncanny coincidences involving those acts and the lives of the flamboyant David Bowie and the ultra-square Al Gore. Consider these "stranger than fiction" parallels:

- Within roughly a 12-month period in 1947 and 1948, both David Robert Jones (later known as David Bowie) and Albert Arnold "Al" Gore, Jr. were born.

- In the 1970s, Bowie morphed into Ziggy Stardust, becoming arguably the greatest rock star of the decade, while simultaneously Congressman Gore was the lone voice in Congress promoting the "fascination[1]" of high-speed telecommunications as an engine for economic growth.

- The National Conference of Commissioners on Uniform State Laws (nka the Uniform Law Commission) finalizes the Uniform Durable Power of Attorney Act in 1979, as David Bowie completes his Berlin Trilogy and Al Gore serves his second term in the House of Representatives.

- In 1986, Congress enacts the Electronic Communications Privacy Act[2] (the "ECPA") and the Computer Fraud and Abuse Act[3] (the "CFAA"); Bowie stars in Jim Henson's cult classic *Labyrinth* as Jareth, the Goblin King; and Gore introduces the Supercomputer Network Study Act of 1986.

- The World Wide Web is invented in 1989, just as Bowie and his new band Tin Machine release their self-titled debut album, a copy of which was undoubtedly purchased by Tipper Gore so that her Parents Music Resource Center could review its lyrics.

- In another 12-month span in 1991-1992, the computer service Prodigy allows subscribers to send 30 free emails per month, Gore drafts the *High Performance Computing Act of 1991* (commonly referred to as "The Gore Bill")[4], and Bowie asks supermodel Iman to "be my wife[5]."

- As a result of Gore's 1993 call for the creation of a "nationwide information superhighway," Mosaic (later Netscape) is released, sparking the Internet boom of the 1990s, increasing the "speed of life[6]" for all of us.

- In 1996 and 1997, while Gore is serving in two important positions—Vice President of the United States and President of the Senate—Bowie receives two important awards: he is inducted into the Rock and Roll Hall of "Fame,[7]" and he receives a star on the Hollywood Walk of Fame.

- Responding to Gore's call, in 1998, Bowie launches BowieNet[8], the first artist-created Internet service provider, and the next year he releases the first album by a major artist available for download prior to its physical release. A press release from the U.K. said it was "logical" that Bowie would be on the cutting edge of digital development.

- In 2006, UPOAA is put in final form by the Uniform Law Commission, Bowie is honored with the Grammy Lifetime Achievement Award and appears in Christopher Nolan's thriller *The Prestige*, and Gore's Academy Award winning film *An Inconvenient Truth* is released.

- In 2007, Steve Jobs introduces Apple's "savior machine[9]," the iPhone, launching the mobile revolution; Al Gore is awarded the Nobel Peace Prize; and Bowie takes some well-deserved time off.

- Realizing that "love is lost[10]," Al and Tipper Gore split in 2010.

- "Where are we now[11]?" In 2016, Gore decided not to run for President again, and a mere 12 days after Bowie's death, Apple refused to give a widow her dead husband's Apple ID without a court order so she could continue to play a bridge game they had purchased using their joint iTunes account.[12]

As fun and interesting (or not) as these facts might be, they have been listed primarily to make some important points. First, as will be discussed more thoroughly below, the two federal acts that have been causing most of the trouble regarding fiduciary access to digital assets were enacted in 1986, several years before the invention of the World Wide Web and social media, and well before virtually anyone actually owned any digital assets. Second, as recent as UPOAA is, that Act was finalized the year before the launch of the iPhone and the subsequent boom in the growth of social media. Third, David Bowie was a visionary, both musically and digitally, who will be missed. Fourth, while Al Gore can claim only partial credit for creating the Internet[13], he was another of "the dreamers[14]," being one of the first to realize the possibilities of computers in the information age, and he crafted at least two of the earliest bills to help foster its growth. Let's "move on[15]."

"Tomorrow belongs to those who can hear it coming." —David Bowie

Tomorrow is coming, and Ohio estate planners hear it. Digital assets are all around us, and they are becoming increasingly important to our clients and their beneficiaries.

Planning for fiduciaries to access those assets is becoming increasingly important as well. If Ohio enacts the UFADAA, part of that enactment is expected to be an OSBA Estate Planning, Trust and Probate Law ("EPTPL") Council proposal to modify Ohio's statutory power of attorney form to make it possible to grant digital asset powers and to permit agents to access electronic communications of their principals. This article will discuss the background problems that agents currently have in dealing with digital assets, the proposed statutory changes, and best practices for counselling clients in dealing with digital asset issues with powers of attorney.

UPOAA Adequately Deals with Digital Assets, Doesn't It?

"If it works, it's out of date." —David Bowie

It's the same old problem all over again. Life comes at us and our clients in the form of the "really real," but the "law[16]" exists only as an abstraction and despite all best attempts, no abstraction can ever adequately deal with all real-life situations. As Yogi Berra once said, "It's like *déjá vu* all over again." The UPOAA seems, and was intended, to grant to agents all authority necessary to deal with digital assets of their principals. UPOAA's official comment to its Section 203 [R.C. 1337.44] states:

> Paragraphs (8) and (9) [i.e. R.C. 1337.44 {K} and {L}] were added to the section to clarify that this comprehensive authority includes authorization to communicate with government employees on behalf of the principal, to access communications intended for the principal, and to communicate on behalf of the principal *using all modern means of communication.* [Emphasis added.]

UPOAA came into existence well into the digital age, but before the advent of the mobile revolution, and it was drafted taking into account the need of agents to be able to access digital records of their principals. In fact, the so-called "referred" or "implied" powers of R.C. § 1337.44 expressly grant to agents the power to "access communications intended for, and communicate on behalf of, the principal, whether by mail, electronic transmission, telephone, or other means" with respect to each statutory power granted by the principal. Moreover, UPOAA and UFADAA share the same definitions for "electronic" and "record," so nothing more should be needed. "Would that it were so simple.[17]"

While UPOAA arguably grants agents the authority necessary to access digital records, an agent attempting to access certain electronic communications of the principal can expect significant obstacles. Moreover, the term "digital assets," which is not defined by UPOAA, encompasses far more than electronic records.

> "Digital assets" include electronically stored information, Internet domain names, virtual currencies like Bitcoin, and online accounts such as email accounts, social networking accounts, banking and investment accounts, shopping accounts, Web pages,

> blogs, photo-sharing accounts, video-sharing accounts, video game accounts, file storage accounts, and more.[18]

Despite the clear intent of UPOAA, if Ohio enacts UFADAA, changes will also be made to the Ohio version of UPOAA to take full advantage of the digital access afforded by UFADAA. This is not because of any deficiency with UPOAA itself, but because of what is almost certainly an unintended interpretation of two federal laws passed in 1986.

Federal Law Complications

"*Turn and Face the Strange*" —David Bowie

Many technology companies take the position that they cannot release information regarding their customer's accounts to fiduciaries because of two federal laws—the Electronic Communications Privacy Act[19] (the "ECPA") and the Computer Fraud and Abuse Act[20] (the "CFAA"). ECPA was a 1986 amendment to the Omnibus Crime Control and Safe Streets Act of 1968 (sometimes referred to as the Wiretap Act), and its primary purpose was to extend government restrictions on wiretaps from telephone calls to include electronic data by computer. CFAA, which was also passed in 1986, is aimed primarily at criminalizing the hacking of computers of the federal governmental and financial institutions.[21] It is clear that neither act sought to limit fiduciary access to digital assets, but because it has been held that any device capable of being connected to the Internet is a protected computer under CFAA,[22] it is "little wonder[23]" that the position of many tech companies has become intransigent. Fortunately, this problem is less common "outside[24]" Silicon Valley.

Much has been written about problems raised by the ECPA and the CFAA with regard to fiduciary access to electronic communications.[25] The former prohibits providers of electronic communications services from disclosing the contents of electronic communications,[26] unless one of eight exceptions applies, and under the latter, the government may charge a person with a crime when that person exceeds authorized access to a digital account.[27] The two ECPA exceptions applicable to agents under powers of attorney are:

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> * * *
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service.

In the context of powers of attorney, under both ECPA and CFAA, an agent needs "authorization" to access the principal's account, and under ECPA's third (but not the first) exception, the provider may only disclose the contents of the communication with the "lawful consent" of the principal (assuming that the principal was the originator or the intended recipient); otherwise, the custodian can only release information about the principal's account. Neither "authorization" nor "lawful consent" is defined.[28]

An agent who, with the principal's consent, uses the principal's password to access the principal's account may commit a crime under CFAA if the Terms of Service ("TOS") agreement of the service provider prohibits the sharing passwords or otherwise prohibits anyone other than the owner from accessing the account.

> The U.S. Department of Justice asserts that § 1030(a)(2) of the Computer Fraud and Abuse Act is broad enough to permit the government to charge a person with a crime for violating the CFAA when that person "exceeds authorized access" by violating the access rules of a Website's Terms of Service contract or use policies. This position was stated by Richard Downing, Deputy Chief of the DOJ's Computer Crime and Intellectual Property Section, Criminal Division, in testimony presented on November 15, 2011, before the U.S. House Committee on Judiciary, Subcommittee on Crime, Terrorism, and National Security. However, Mr. Downing also testified, "Let me be very clear that the DOJ is in no way interested in bringing cases against the people who lie about their age on a dating site or anything of the sort. We don't have time or resources to do that."[29]

Applying a 1986 cybercrime bill to an agent with digital-asset powers for accessing the Facebook or Gmail account of the principal in violation of the TOS makes as much sense as interpreting the Second Amendment—drafted at a time when the only guns available were front-end muzzle loaders—as protecting the right to own privately and to

carry openly automatic assault rifles capable of shooting 600 rounds a minute. Yet that is where we are, in both cases, making us feel "unwashed and somewhat slightly dazed[30]." "*Speak in extremes, it'll save you time.*" —David Bowie

Here's "what's really happening[31]." A reasonable interpretation of ECPA, as well as its legislative history,[32] both allow fiduciaries to be able to step into the shoes of the account holder whose interests the fiduciary represents; however, many tech companies assert that the prospect of fines under ECPA and the threat of criminal sanctions under CFAA make them "tumble and twirl[33]" forcing them to interpret those acts in the most restrictive way possible to protect themselves from potential liability.

In this regard, agents under powers of attorney appear to be in a better position than any other fiduciary, because the ECPA permits the custodian of electronic communications to divulge the contents to the intended recipient of the communication *or to the intended recipient's agent*. Three things should be noted. First, this merely permits the custodian to reveal the contents of the communication; the custodian cannot be compelled by anyone to release the communication. Secondly, the contents can only be released to the agent *of the recipient*, not to the agent of a sender. While it might be criminal for an agent to access the account because, for example, the TOS limits access solely to the account owner, the service provider is permitted to give the agent the contents of communication sent to (but not sent by) the account owner. In other words, an agent attempting to access the email account of his or her principal would only be permitted to access the inbox, but not the "sent" folder! Third, ECPA exceptions (1) and (3) significantly overlap; however (3) requires "lawful consent" while (1) does not.

UPOAA is Getting an Upgrade

"*Ch-ch-ch-ch-Changes.*" —David Bowie

To overcome the purported challenges posed by federal law and to fully avail an agent of the powers granted by UFADAA, the EPTPL Council has proposed two revisions to UPOAA.

The first proposed revision to UPOAA defines an agent's digital-asset powers by adding a new section to Revised Code Chapter 1337. UFADAA lists those things that a power of attorney can authorize an agent to do, but it remains necessary for the power of attorney document to actually grant those powers. Accordingly, the EPTPL Council chose to assemble the five things that UFADAA permits an agent to do into one digital asset power. Defining an agent's digital-asset powers in this way will make it easy for principals to authorize their agents to do everything agents are permitted to do under UFADAA. The proposed new section reads as follows:

> Unless the power of attorney otherwise provides, language in a power of attorney granting general authority with respect to digital assets causes the agent to be an authorized user for the purpose of applicable computer fraud and unauthorized computer access laws and authorizes the agent to do all of the following:
>
> (A) have access to any catalog of electronic communications sent or received by the principal;
> (B) have access to any other digital asset in which the principal has a right or interest;
> (C) have the right to access any of the principal's tangible personal property capable of receiving, storing, processing, or sending a digital asset;
> (D) take any action concerning the asset to the extent of the account holder's authority;
> (E) have access to the content of electronic communications sent or received by the principal.

The new section will mesh well with UPOAA's existing provisions. Revised Code § 1337.44 allows a principal to grant many powers to an agent with respect to various subject matters by referencing one or more subjects listed in Revised Code §§ 1337.45-58. Consolidating digital-asset powers into one subject-matter section means a principal will be able to grant all of these powers by reference to the digital asset powers without having to list the five digital asset powers individually in the power of attorney.[34]

The second revision to the statutory power-of-attorney form in Revised Code § 1337.60 is the addition of two new lines which the principal can initial. The first of these is to grant the statutory digital assets powers referred to in the preceding paragraph. By initialing the second new line, the principal indicates consent to the release of the content of electronic communications to the agent. As discussed above, exception (3) to the ECPA's

prohibition of release of the content of electronic communications allows the release with the "lawful consent" of the originator or recipient. It was the Council's belief that lawful consent, whatever that might mean, likely cannot be granted by means of a statutory definition of digital asset powers, but instead probably requires the actual consent of the principal. The proposed UPOAA statutory definition of digital-asset powers includes authorization for the agent to access the content of electronic communications, but it is not clear whether referring to the statute will be sufficient to shelter the agent and the digital account custodian from liability. Including an express grant of authority in the power of attorney should satisfy the lawful consent requirement, thereby allowing the custodian to release the content of the communication to the agent without facing the prospect of significant liability under CFAA.

What Can My Clients and I Do Until UFADAA Passes?

"*I can see light at the end of the tunnel and it isn't a train.*" —David Bowie

"*I've come to the realizations that I have absolutely no idea what I'm doing half the time.*" —David Bowie

Grant the Digital-Asset Powers Now. Clients will not need to execute new powers of attorney following enactment of UFADAA if they include the proposed statutory power in their power of attorney documents now. If the statutory form is used, the grant of this power should be set forth under the section entitled "Special Instructions." The suggested form is:

> My agent shall have the authority with respect to digital assets to exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of any kind of computing device of mine, any kind of data storage device or medium of mine, any electronically stored information of mine, any user account of mine; and any domain name of mine. Specifically, my agent shall (1) have access to any catalog of electronic communications sent or received by me, (2) have access to any other digital asset in which I have a right or interest, (3) have the right to access any of my tangible personal property used to store any of my digital assets, (4) have the power to take any action concerning the asset to the extent of my authority, and (5) have access to the content of electronic communications sent or received by me. This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law.

Second, the principal should authorize third parties with whom the principal maintains accounts to release information to the agent. UFADAA will provide for that authorization, but until its enactment, the better practice might be to have clients sign separately a broad authorization, as set forth below, simply because some tech companies seem incapable of understanding the concept that P authorizing A to access P's electronic communications necessarily includes P's consent to the disclosure of those communications to A. Many providers will accept the agent's authority to deal with digital assets if a grant of that power is set forth in the power of attorney. For those who will not, a copy of the authorization could be provided. A suggested form (which addresses the release of information to the agent and other fiduciaries) is:

> I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my then-acting fiduciaries at any time: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. The terms used in this authorization are to be construed as broadly as possible, and the term "fiduciaries" includes an agent acting under a power of attorney signed by me, a guardian appointed for me, a trustee of my revocable trust, and the executor of my estate. This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and any other applicable federal or state data privacy law or criminal law. This authorization is effective immediately. Unless this authorization is revoked by me in writing while I am competent, this authorization continues to be effective during any period that I am incapacitated and continues to be effective after my death. Unless a person or entity has received actual notice that this authorization has been validly revoked by me, that person or entity receiving this authorization may act in reliance on the presump-

> tion that it is valid and unrevoked, and that person or entity is released and held harmless by me, my heirs, legal representatives, successors, and assigns from any loss suffered or liability incurred for acting according to this authorization. A person or entity may accept a copy or facsimile of this original authorization as though it were an original document.[35]

Educate the Client. Many clients do not recognize the value of their digital assets. Assets with little perceived worth (such as a 10-year-old Toyota Corolla their son drives, a seldom-used bank account that contains only a couple of thousand dollars, or a "small plot of land[36]") are often not volunteered by clients in a discussion of their assets.

Because most clients are looking for a "miracle goodnight[37]" rather than a host of post-incapacity or death problems, a short discussion about how a low-value asset can trigger the need for probate estate administration often opens their eyes from their "moonage daydream[38]" making them realize the importance of properly planning for all of their assets—not just the ones they perceive to be the most valuable.

Saying, "I keep forgettin'[39]" a typical client will often fail to mention digital assets the value of which is primarily sentimental, assuming that we, as planners, are only concerned with assets having financial value. Clients need to provide for access to their terabytes of pictures on Flickr or their thoughts and impressions of daily life in their Gmail and Facebook (but probably not Ashley Madison) accounts, upon their disability or death.

Discuss with clients what data they would regret losing if their computer, mobile phone, or other device were to be lost or destroyed, and what information on those devices might be critically important to their agents in the event of their incapacity. Undoubtedly, "some are[40]" already thinking about this.

Clients Must Inventory Their Digital Assets. Clients should be asked to make a list of all of their electronic devices, email addresses, personal websites, social media sites, cloud-storage services, media-sharing sites, banking and brokerage accounts, and the usernames, passwords, and security questions and answers for each. A good template is Minneapolis Attorney Jim Lamm's Digital Audit form.[41] Because such a list contains so much sensitive information, it should be kept in a secure location able, and the agent to whom the digital asset powers are granted should be aware of the existence and location of the list.

Tech-savvy clients should be encouraged to use password-management software (e.g., LastPass or Dashlane), which stores usernames and passwords in a digital "vault" that is unlocked by us-ing a master password. The vault can be often synchronized across devices and operating systems to make accessing passwords convenient as well as secure. Some pass-word-management software has the option to allow the software to "autofill" usernames and passwords, which is faster than reviewing a printed list and less tedious than typing the (ideally) secure password into the website.

Even though the password vault is secure, the master password along with instructions on how to access the password vault should be locked away. As with a physical listing of the principal's digital inventory, the agent to whom the digital asset powers are given must be able to access the password vault, if and when it becomes necessary for the agent to act.

Clients Must Use Strong, Unique Passwords and Update Them Regularly. Once your clients' usernames and passwords have been cataloged, it is important that they are kept updated. While many corporate IT procedures require passwords to be changed at regular intervals, few Websites have such a requirement. Still, changing passwords to Websites periodically is wise because it reduces the risk that a password will be compromised. Two password managers, LastPass and Dashlane, make this process easy by updating your passwords on many popular Websites with a few clicks.[42] Other similar programs are available, and we should tell our clients to "try some, buy some[43]." Clifford Stoll, who is known for his pioneering work in computer counter-espionage, offers a good rule of thumb: "Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months."

Strong passwords are critical. Generally, a strong

password should be eight characters long or longer, not contain any words or names, include at least one capital letter, one lower-case letter, one number, and one special character (such as an asterisk or ampersand), and be is significantly different from prior passwords for that site.[44] Using password-management software that has an autofill feature eliminates the downside of long, complicated passwords. Many password managers will also generate strong passwords for you, which makes long, strong passwords easier than shorter, less-secure ones that you create yourself.

Using unique passwords on each Website reduces the risk that a compromised password will have catastrophic results. In 2010, the New York Times reported that hackers stole 32 million passwords from an online gaming company, and that of those stolen, 20% (about 6,400,000) shared 5,000 common passwords.[45] For a user who also utilizes one common password on multiple sites, the cost of that data breach would be much higher than for a user committed to using a unique password for each account.

Clients whose passwords are secured using a password manager should be periodically reminded to update the master password. A hard copy should be kept in a secure place like a safe, to which the agent has access.

Clients Should Use Multi-Factor Authentication. Accounts that require multi-factor authentication ("MFA"—sometimes called two-factor authentication) need more than just a password to obtain access. A password is one factor, and the second factor is often a one-time-use code. The code might be sent by email or text (to a pre-approved phone number), or it might be generated by a computer or smartphone app (e.g., Authy or Google Authenticator). Even if a client's password is stolen or breached, an account protected by MFA may still be secure.

Clients with MFA accounts must be sure their agents have access to their computers, phones, and other devices or the agents may be shut out of certain accounts despite having the password.

Attorneys Should Not Keep Clients' Passwords. Attorneys should generally not offer to keep a copy of a client's passwords. An attorney's files may seem like an ideal place to keep passwords, but if a password is compromised, the attorney may face allegations that he or she disclosed a password to someone other than the client.

The only time an attorney should consider keeping a client's password is if the account for that password is also secured by multi-factor authentication in addition to the password.

Clients Should Regularly Backup Their Digital Assets. Important information (whether on a computer, smartphone, or other device) should be regularly backed up. The fastest, most cost-effective solution is physical storage in the client's possession (e.g., external hard drive, DVD, or flash drive), but this method is often subject to the same risks as the original source. Floods, fires, and theft can result in the loss of both the original data and the backup. While online backup services are typically slower, the fact that the physical servers will located at a distant location virtually assures that the backup will not be susceptible to the same risks as the original data. The best backup plan is one that incorporates both local media and online services.

Name the "Right[46]" Agent. Many clients name as their agent someone who lacks even the most rudimentary computer skills. Dealing with online custodians of digital accounts can be expected to present challenges for any agent, and those challenges could well be insurmountable if the wrong agent is selected. In these cases, consideration should be given to suggesting to the client that a separate power of attorney be executed that deals with the digital powers only, appointing an agent who would have a higher degree of competence in dealing with digital assets.

Act Quickly Upon Incapacity. An agent may need to act quickly upon the principal's disability. Many free online email services delete accounts following relatively short periods of inactivity. Some clients use email folders as their filing system for important information, and a review of the content of emails is sometimes the only way to learn of the existence of intra-family loans or of the amounts currently owed on such loans—information that

could be of critical importance following the principal's death. It is virtually impossible to determine what might be important later on or after the principal's death, so the agent may want to backup all email records quickly. Many clients do not keep paper copies of bank or brokerage account statements, relying upon their ability to access those statements online. Many financial institutions only provide access to a limited number of prior account statements (e.g., for the last 12 months), so the agent may want to download those statements while they are still available. It is the authors' opinion, and apparently the opinion of the Justice Department's Computer Crime and Intellectual Property Section,[47] that an agent to whom digital assets powers have been granted would not be subjected to liability under either federal statute for logging onto the principal's account with the principal's password, even if that violated the TOS of the provider. The more practical concern would be that such a violation could result in the provider terminating the account.

When an agent begins to act following the principal's lack of capacity, it is no longer sufficient to go through the principal's mail or desk drawers looking for unpaid bills or records of financial accounts. Many, if not most, of those types of things that previously had a paper trail now exist primarily or solely in digital form. Without access to the principal's email account, many bills may go unpaid. Without having access to the principal's computer and account passwords, the agent will not be able to access those financial accounts that exist primarily on the Internet.

When an Internet-capable device is connected to an account, at least two computers are involved—those of the account owner (e.g., the principal's laptop) and of the service provider. CFAA arguably requires that the agent accessing the account have authority to access the computer on each end. The principal can clearly grant to the agent authority to access her computer, but only the service provider can grant authority to access its server. That authorization is often denied by Terms of Service agreements.

> For example, Facebook's TOS provides that "[y]ou will not solicit login information or access an account belonging to someone else." So, although the account holder may authorize the fiduciary to access the account, the fiduciary may be exceeding authorized access—within the meaning of the CFAA—by logging into the Facebook account if that access violates Facebook's TOS.[48]

While UFADAA will likely resolve this problem at both ends, it is possible that amendments may be needed to both ECPA and CFAA. While there is a "sense of doubt[49]" about whether or not UFADAA completely provides everything that is needed to ensure fiduciary access, a totally complete solution would also involve amendments to these two pre-Internet acts. ECPA should be amended to add a ninth exception listing fiduciaries as permissible recipients of the contents of communications and both ECPA and CFAA should be amended to define "authorization" in a way that permits fiduciaries to grant the required consent.

Conclusion

"*The last thing you should do.*" —David Bowie

If we are looking for "a new career in a new town[50]," it is estate planning for digital assets, and as estate planners, we are "under pressure[51]" to help our clients plan for the disposition of their digital assets in addition to the usual mix of real and personal property. As is all too often the case, the law lags far behind societal trends, as evidenced by the application of pre-Internet federal law to online accounts. Fortunately, UFADAA brings us a world of "wishful beginnings[52]," lighting the way forward so that problems with the major tech companies should "slip away[53]" The proposed Ohio modifications to our enactment of UPOAA arm agents with the fullest level of authority permitted by the new act. But that is not enough. As estate planners, we need to make sure that our clients who are entering their "golden years[54]" understand the scope of the issues presented by digital assets and provide them and their designated decision makers with the tools necessary to preserve and to pass to others all that will remain behind—their digital footprints: "here today and gone tomorrow[55]."

ENDNOTES:

[1]Fascination, from Bowie's 1975 album *Young*

Americans

[2]18 U.S.C. 2510.

[3]18 U.S.C. 1030. Title 2 of ECPA is referred to as the Stored Communications Act.

[4]"Among the many technological achievements that resulted from the funding of the Gore Bill, was the development of Mosaic in 1993, the World Wide Web browser software which is credited by most scholars as beginning the Internet boom of the 1990s." *Wikipedia* article on High Performance Computing Act of 1991.

[5]"Be My Wife," a single released by Bowie in 1977.

[6]"Speed of Life" was Bowie's first instrumental and is in his 1977 album *Low*.

[7]"Fame" was recorded by Bowie and released in 1975.

[8]For $19.95 per month, users got a yourname@davidbowie.com email address, 5MB of online storage to create a personal web page, access to exclusive audio and video, and a chat room which included live chats with Bowie himself.

[9]"Saviour Machine" is from Bowie's 1970 album *The Man Who Sold the World*.

[10]"Love Is Lost" is from Bowie's album *The Next Day*.

[11]"Where Are We Now?" is the first track on Bowie's 2013 album, *The Next Day*.

[12]"Widow who wanted her dead husband's Apple ID so she could play games on their iPad is refused and told to get a COURT order instead," DailyMail.com, January 20, 2016.

[13]See Stix, Gary, "Gigabit Gestalt: Clinton and Gore Embrace an Activist Technology Policy," Scientific American, (May 1993, at 122-126).

[14]"The Dreamers" is the 10th track on Bowie's 1999 album, *Hours*, which has the distinction of being the first complete album by a major artist available for download over the Internet prior to its physical release.

[15]"Move On" is from Bowie's 1979 album *Lodger*.

[16]"Law (Earthings on Fire)" is from Bowie 1997 album Earthlings.

[17]Spoken by the character Hobie Doyle, in the Coen Brothers film Hail, *Caesar* 2016. See https://www.youtube.com/watch?v=kGpsXuMvApo.

[18]From a January 28, 2015 ACTEC letter to the Senate Subcommittee on Privacy, Technology and the Law and the House Subcommittee on Courts, Intellectual Property, and the Internet.

[19]18 U.S.C. 2510.

[20]18 U.S.C. 1030. Title 2 of ECPA is referred to as the Stored Communications Act.

[21] The focus of CFAA was the prevention of cybercrime against federal computers and bank computers, by proscribing unauthorized disclosure of protected information related to "national defense or foreign relations," "restricted data. . . as defined in . . . of the Atomic Energy Act," "information that . . . could be used to the injury of the United States." CFAA also prohibits the unauthorized access of financial records of financial institutions or from any department or agency of the United States. Only incidentally does the CFAA prohibit unauthorized access to "information from any protected computer."

[22]A protected computer is defined as a computer "which is used in or affecting interstate or foreign commerce," which in turn has been judicially construed as any electronic device capable of being connected to the Internet. *United States v. Mitra*, 405 F.3d 492, 495-96 (7th Cir. 2005), aff'd, 134 F. App'x 963 (7th Cir. 2005), cert. denied sub nom. In *Mitra v. United States*, 546 U.S. 979 (2005), the Court held that any instrument capable of accessing the Internet, including cell phones and iPods, falls within the definition of "computer" under the CFAA.

[23]Little Wonder" is from Bowie's 1997 album *Earthling*.

[24]"Outside" is the title of a Bowie 1995 concept album.

[25]For a detailed discussion of this issue, see *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, James D. Lamm, Christina L. Kunz, Damien A. Riehl, and Peter John Rademacher, *University of Miami Law Review*, Vol. 68, 385.

[26]18 U.S.C. § 2702(a) prohibits a provider of an electronic communication and computing services from knowingly divulging the contents of a person's electronic communications.

[27] 18 U.S.C. § 1030 provides:

> (a) Whoever
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (C) information from any protected computer;
>
> shall be punished as provided in subsection (c) of this section.

[28]*LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009) interpreted "authorization" as meaning any permission at all.

[29]*Digital Passing: Oh, What a Tangled Web We Weave*, James D. Lamm, 58th Annual Estate Planning Seminar, Seattle, WA (Oct. 21, 2013).

[30]Unwashed and Somewhat Slightly Dazed" is from Bowie's 1969 album *David Bowie*.

[31]"What's Really Happening?" is from Bowie's 1999 album *Hours*.

[32]In Senate Report 99-541 from the Committee

on the Judiciary, the analysis of § 2702 states the following:

The exceptions to the general rule of nondisclosure provided in subsection (b) fall into three categories. The first category are those disclosures which are authorized by either the sender or receiver of the message. Either the sender or the receiver can directly **or through authorized agents** authorize further disclosures of the contents of their electronic communication. (Emphasis added.)

[33]"Tumble and Twirl" is from Bowie's 1984 album *Tonight*.

[34]Access to the content of the principal's electronic communications should be expressly granted in the power of attorney because it is not clear whether reference to the statutory section is sufficient to comply with federal law.

[35]*Supra*, n. 12, at pages 418-9, with minor revisions tailoring the provision to Ohio law.

[36]"A Small Plot of Land," is from Bowie's 1995 album *Outside*.

[37]"Miracle Goodnight" is from Bowie's album *Black Tie White Noise*.

[38]"Moonage Daydream" is a Bowie song from his 1972 breakout album *The Rise and Fall of Ziggy Stardust and the Spiders from Mars*.

[39]David Bowie recorded a version of the song for his 1984 album *Tonight*.

[40]"Some Are" is a song by Bowie recorded during the *Low* sessions in 1976 and released as a bonus track on the release of *Low* in 1991.

[41]Available at http://www.digitalpassing.com/wordpress/wp-content/uploads/2012/08/DigitalAudit.pdf.

[42]Paul, Ian, "How to change your passwords automatically with Dashlane and LastPass," *MacWorld*, May 6, 2016, accessible at http://www.macworld.com/article/3065969/security/how-to-change-your-passwords-automatically-with-dashlane-and-lastpass.html#tk.rss__all.

[43]"Try Some, Buy Some" is a 1971 George Harrison song. A longtime admirer of the song, Bowie version is in his 2003 album *Reality*.

[44]"Tips for creating a strong password," accessible at http://windows.microsoft.com/en-US/windows-vista/Tips-for-creating-a-strong-password.

[45]*Id*.

[46]"Right" is a song from Bowie's 1975 album *Young Americans*.

[47]See n. 16, *supra*.

[48]*Supra*, n. 12, at page 401.

[49]"Sense of Doubt" is an instrumental piece written by Bowie for his 1977 album *Heroes*.

[50]"A New Career in a New Town" is an instrumental piece by Bowie from his 1977 album *Low*.

[51]"Under Pressure" is a 1981 song originally recorded by Queen and David Bowie, and later included on Queen's 1982 album *Hot Space*.

[52]"Wishful Beginnings" if from the 1995 album *Outside*.

[53]"Slip Away" is Bowie's homage to New Jersey "Uncle" Floyd Vivino, a vaudeville-styled comedian.

[54]"Golden Years" is from Bowie's 1975 album *Station to Station*.

[55]"Here Today and Gone Tomorrow" was not written by Bowie, but he performed it on his Diamond Dogs tour in 1974, and it was released as a bonus track on the 1990 Rykodisc reissue of the live album *David Live*.

WILLS AND TRUSTS: UPDATING OHIO'S PRE-MORTEM VALIDATION LAW

By Ralph Lehman, Esq.

Logee, Hostetler, Stutzman & Lehman
Wooster, Ohio
Chairman, EPTPL Committee for Validation of Wills and Trusts Before Death

Currently, Ohio law allows a living testator to have the probate court determine if the testator's will is valid and, if determined to be valid, to prevent a post-death challenge to the will. The Estate Planning, Trust and Probate Law Section of the Ohio State Bar Association (OSBA) has proposed modifications to the procedure, and to allow a similar procedure for trusts.

The proposal would replace Sections 2107.081 to 2107.085 of the Revised Code with Chapter 5817 of the Revised Code.

Current Ohio Law. Ohio's current pre-mortem statute provides that:

- The complaint must be filed in the probate court located in the testator's county of domicile and, if not domiciled in Ohio, the county in which any of the testator's real property is located.[1]
- The complaint must name the following as defendants: beneficiaries under the will, and those who would inherit if the testator died on the date the complaint is filed.[2]
- After notice to all defendants, the court conducts a hearing.[3]

