

CYBER ESTATE PLANNING AND ADMINISTRATION



GERRY W. BEYER

*Governor Preston E. Smith Regents Professor of Law
Texas Tech University School of Law
Lubbock, TX 79409*

*(806) 834-4270
gwb@ProfessorBeyer.com
<http://www.ProfessorBeyer.com>
<http://www.BeyerBlog.com/>*

SIOUX FALLS ESTATE PLANNING COUNCIL

Sioux Fall, South Dakota

June 15, 2016

GERRY W. BEYER

**Governor Preston E. Smith Regents Professor of Law
Texas Tech University School of Law
Lubbock, TX 79409-0004
(806) 834-4270
gwb@ProfessorBeyer.com – www.ProfessorBeyer.com**

EDUCATION

B.A., Summa Cum Laude, Eastern Michigan University (1976)
J.D., Summa Cum Laude, Ohio State University (1979)
LL.M., University of Illinois (1983)
J.S.D., University of Illinois (1990)

SELECTED PROFESSIONAL ACTIVITIES

Bar memberships: United States Supreme Court, Texas, Ohio (inactive status), Illinois (inactive status)
Member: American Law Institute; American College of Trust and Estate Counsel (Academic Fellow); American Bar Foundation; Texas Bar Foundation; American Bar Association; Texas State Bar Association
Editor-in-Chief, REPTL Reporter, State Bar of Texas (2013-present)
Keeping Current Probate Editor, *Probate and Property* magazine (1992-present)

CAREER HISTORY

Private Practice, Columbus, Ohio (1980)
Instructor of Law, University of Illinois (1980-81)
Professor, St. Mary's University School of Law (1981-2005)
Governor Preston E. Smith Regent's Professor of Law, Texas Tech University School of Law (2005 – present)
Visiting Professor, Boston College Law School (1992-93)
Visiting Professor, University of New Mexico School of Law (1995)
Visiting Professor, Southern Methodist University School of Law (1997)
Visiting Professor, Santa Clara University School of Law (1999-2000)
Visiting Professor, La Trobe University School of Law (Melbourne, Australia) (2008 & 2010)
Visiting Professor, The Ohio State University Moritz College of Law (2012)
Visiting Professor, Boston University School of Law (2014)

SELECTED HONORS

Order of the Coif
Estate Planning Hall of Fame, National Association of Estate Planners & Councils (2015)
ABA Journal Blawg 100 Hall of Fame (2015)
Outstanding Professor Award – Phi Alpha Delta (Texas Tech Univ.) (2016) (2015) (2013) (2010) (2009) (2007) (2006)
Excellence in Writing Awards, American Bar Association, Probate & Property (2012, 2001, & 1993)
President's Academic Achievement Award, Texas Tech University (2015)
Outstanding Researcher from the School of Law, Texas Tech University (2013)
Chancellor's Council Distinguished Teaching Award (Texas Tech University) (2010)
President's Excellence in Teaching Award (Texas Tech University) (2007)
Professor of the Year – Phi Delta Phi (St. Mary's University chapter) (1988) (2005)
Student Bar Association Professor of the Year Award – St. Mary's University (2001-2002) (2002-2003)
Russell W. Galloway Professor of the Year Award – Santa Clara University (2000)
Distinguished Faculty Award – St. Mary's University Alumni Association (1988)
Most Outstanding Third Year Class Professor – St. Mary's University (1982)
State Bar College – Member since 1986

SELECTED PUBLICATIONS

Author and co-author of numerous law review articles, books, and book supplements including WILLS, TRUSTS, AND ESTATES: EXAMPLES AND EXPLANATIONS (6th ed. 2015); FAT CATS AND LUCKY DOGS – HOW TO LEAVE (SOME OF) YOUR ESTATE TO YOUR PET (2010); TEACHING MATERIALS ON ESTATE PLANNING (4th ed. 2013); 9 & 10 TEXAS LAW OF WILLS (Texas Practice 2002); TEXAS WILLS AND ESTATES: CASES AND MATERIALS (7th ed. 2015); 12, 12A, & 12B WEST'S TEXAS FORMS — ADMINISTRATION OF DECEDENTS' ESTATES AND GUARDIANSHIPS (3rd ed. 2007); *When You Pass on, Don't Leave the Passwords Behind: Planning for Digital Assets*, PROB. & PROP., Jan./Feb. 2012, at 40; *Wills Contests – Prediction and Prevention*, 4 EST. PLAN. & COMM. PROP. L.J. 1 (2011); *Digital Wills: Has the Time Come for Wills to Join the Digital Revolution?*, 33 OHIO N.U.L. REV. 865 (2007); *Pet Animals: What Happens When Their Humans Die?*, 40 SANTA CLARA L. REV. 617 (2000); *Ante-Mortem Probate: A Viable Alternative*, 43 ARK. L. REV. 131 (1990).

TABLE OF CONTENTS

I. INTRODUCTION	1
II. TYPES OF DIGITAL ASSETS.....	1
A. Personal.....	1
B. Social Media	2
C. Financial Accounts	2
D. Business Accounts.....	2
E. Domain Names or Blogs	2
F. Loyalty Program Benefits	2
G. Other Digital Assets	2
III. IMPORTANCE OF PLANNING FOR DIGITAL ASSETS.....	3
A. To Make Things Easier on Executors and Family Members.....	3
B. To Prevent Identity Theft.....	3
C. To Prevent Financial Losses to the Estate	3
D. To Avoid Losing the Deceased’s Personal Story.....	4
E. To Prevent Unwanted Secrets from Being Discovered	4
F. To Prepare for an Increasingly Information-Drenched Culture	5
IV. USER AGREEMENTS	5
A. Terms of Service	5
B. Ownership	6
V. FEDERAL LAW	6
A. Stored Communications Act.....	6
B. Computer Fraud and Abuse Act	7
C. Interface With User Agreements.....	7
VI. PLANNING SUGGESTIONS	7
A. Specify Disposition According to Provider’s Instructions	7
B. Back-Up to Tangible Media	8
C. Prepare Comprehensive Inventory of Digital Estate.....	8
D. Provide Immediate Access to Digital Assets.....	9
E. Authorize Agent to Access Digital Assets	9
F. Place Digital Assets in a Trust	9
G. Place Digital Asset Information in a Will.....	9
H. Use Online Afterlife Company	10
VII. OBSTACLES TO PLANNING FOR DIGITAL ASSETS.....	11
A. Safety Concerns	11
B. Hassle	12
C. Uncertain Reliability of Online Afterlife Management Companies	12
D. Overstatement of the Abilities of Online Afterlife Management Companies.....	12

E. Federal Law Restrictions	12
VIII. FIDUCIARY ACCESS TO DIGITAL ESTATE.....	13
A. Existing State Law.....	13
B. Uniform Fiduciary Access to Digital Assets Act	15
C. Privacy Expectation Afterlife and Choices Act.....	17
D. Virginia.....	18
E. Revised Uniform Fiduciary Access to Digital Assets Act	18
F. Cases.....	19
IX. FUTURE REFORM AREAS	19
A. Providers Gather User’s Actual Preferences	19
B. Congress Amends Federal Law	19
C. States Enact RUFADAA	19
X. CONCLUSION.....	20
APPENDIX A – DIGITAL ESTATE INFORMATION SAMPLE FORM.....	21
APPENDIX B – NCCUSL’S COMPARSION OF UFADAA, PEAC, AND RUFADAA	30
POWERPOINT SLIDES.....	35

CYBER ESTATE PLANNING AND ADMINISTRATION

I. INTRODUCTION

For hundreds of years, we have viewed personal property as falling into two major categories – tangible (items you can see or hold) and intangible (items that lack physicality). Recently, a new subdivision of personal property has emerged that many label as “digital assets.” There is no real consensus about the property category in which digital assets belong. Some experts say they are intellectual property, some say they are intangible property, and others say they can easily be transformed from one form of personal property to another with the click of a “print” button. See Scott Zucker, [*Digital Assets: Estate Planning for Online Accounts Becoming Essential \(Part II\)*](#), The Zucker Law Firm PLLC (Dec. 16, 2010). In actuality, some accounts that we consider “assets” are simply licenses to use a website’s service that generally expire upon death. See Steven Maimes, [*Understand and Manage Digital Property*](#), The Trust Advisor Blog (Nov. 20, 2009).

Digital assets may represent a sizeable portion of a client’s estate. A survey conducted by McAfee, Inc. revealed that the average perceived value of digital assets for a person living in the United States is \$54,722. [*McAfee Reveals Average Internet User Has More Than \\$37,000 in Underprotected ‘Digital Assets’*](#), McAfee.com, (Sept. 27, 2011) (the \$37,000 figure is the global average).

While estate planners have perfected techniques used to transfer types of property that have been around for a long time, most estate planners have not figured out how to address the disposition of digital assets. It is important to understand digital assets and to incorporate the disposition of them into clients’ estate plans.

This article aims to educate estate planning professionals on the importance of planning for the disposition of digital assets, provides those planning techniques, and discusses how to administer an estate containing digital assets. The appendix contains a sample form that your clients may use to organize their digital assets.

II. TYPES OF DIGITAL ASSETS

The term “digital asset” does not have a well-established definition as the pace of technology is faster than the law can adapt. One of the best definitions is found in a proposed Oregon statute:

“Digital assets” means text, images, multimedia information, or personal property stored in a digital format, whether stored on a server, computer, or other electronic device which currently exists or may exist as technology develops, and regardless of the ownership of the physical device upon which the digital asset is stored. Digital assets include, without limitation, any words, characters, codes, or contractual rights necessary to access the digital assets.

[*Digital Assets Legislative Proposal*](#), OREGON STATE BAR (May 9, 2012).

Digital assets can be classified in numerous different ways, and the types of property and accounts are constantly changing. (A decade ago, who could have imagined the ubiquity of Facebook? Who can imagine what will replace it in the next few decades?) People may accumulate different categories of digital assets: personal, social media, financial, and business. The individual may also have a license or property ownership interest in the asset. See Laura Hoexter and Alexandra Gerson, [*Who Inherits My Facebook? Estate Planning for Digital Assets*](#) (June 25, 2012). Although there is some overlap, of course, clients may need to make different plans for each.

A. Personal

The first category includes personal assets stored on a computer or smart phone, or uploaded onto a web site such as Flickr or Shutterfly. These can include treasured photographs or videos, e-mails, or even playlists. Photo albums can be stored on an individual’s hard drive or created through an on-line system. (They also can be created through social media, as discussed below.) People can store medical records and tax documents for themselves or family members. The list of what a

client's computers can hold is, almost literally, infinite. Each of these assets requires different means of access—simply logging onto someone's computer generally requires a password, perhaps a different password for operating system access, and then each of the different files on the computer may require its own password.

B. Social Media

Social media assets involve interactions with other people on websites Facebook, MySpace, LinkedIn, and Twitter, as well as e-mail accounts. These sites are used not only for messaging and social interaction, but they also can serve as storage for photos, videos, and other electronic files.

C. Financial Accounts

Though some bank and investment accounts have no connection to brick-and-mortar buildings, most retain some connection to a physical space. They are, however, increasingly designed to be accessed via the Internet with few paper records or monthly statements. For example, an individual can maintain an Amazon.com account, be registered with PayPal, Bitcoin, or other financial sites, have an e-Bay account, and subscribe to magazines and other media providers. Many people make extensive arrangements to pay bills online such as income taxes, mortgages, car loans, credit cards, water, gas, telephone, cell phone, cable, and trash disposal.

D. Business Accounts

An individual engaged in any type of commercial practice is likely to store some information on computers. Businesses collect data such as customer orders and preferences, home and shipping addresses, credit card data, bank account numbers, and even personal information such as birthdates and the names of family members and friends. Physicians store patient information. eBay sellers have an established presence and reputation. Lawyers might store client files or use a Dropbox.com-type service that allows a legal team spread across the United States to access litigation documents through shared folders.

E. Domain Names or Blogs

A domain name or blog can be valuable, yet access and renewal may only be possible through a password or e-mail.

F. Loyalty Program Benefits

In today's highly competitive business environment, there are numerous options for customers to make the most of their travel and spending habits, especially if they are loyal to particular providers. Airlines have created programs in which frequent flyers accumulate "miles" or "points" they may use towards free or discounted trips. Some credit card companies offer users an opportunity to earn "cash back" on their purchases or accumulate "points" which the cardholder may then use for discounted merchandise, travel, or services. Retail stores often allow shoppers to accumulate benefits including discounts and credit vouchers. Some members of these programs accumulate a staggering amount of points or miles and then die without having "spent" them. For example, there are reports that "members of frequent-flyer programs are holding at least 3.5 trillion in unused miles." [*Managing Your Frequent-Flyer Miles*](#) (last visited Oct. 21, 2012). *See also* Becky Yerak, [*Online Accounts After Death: Remember Digital Property When Listing Assets*](#), CHICAGO TRIB., Aug. 26, 2012.

The rules of the loyalty program to which the client belongs plays the key role in determining whether the accrued points may be transferred. Many customer loyalty programs do not allow transfer of accrued points upon death, but as long as the beneficiary knows the online login information of the member, it may be possible for the remaining benefits to be transferred or redeemed. However, some loyalty programs may view this redemption method as fraudulent or require that certain paperwork be filed before authorizing the redemption of remaining benefits.

G. Other Digital Assets

Your client may own or control virtually endless other types of digital assets. For example, your client may own valuable "money," avatars, or virtual property in online games such as World of Warcraft or Second Life.

III. IMPORTANCE OF PLANNING FOR DIGITAL ASSETS

A. To Make Things Easier on Executors and Family Members

When individuals are prudent about their online life, they have many different usernames and passwords for their accounts. This is the only way to secure identities but this devotion to protecting sensitive personal information can wreak havoc on families upon incapacity or death. See Andrea Coombes, [You Need an Online Estate Plan](#), WALL ST. J. July 19, 2009. Consider A&E's *Hoarders*, a reality-based television show that reveals the lives of people who cannot part with their belongings and have houses full of floor-to-ceiling stacks of "junk" as a result. While most of us find this disgusting, are we not also committing the same offense online when we create multiple e-mail accounts, social networking accounts, websites, Twitter accounts, eBay accounts, online bill-paying arrangements, and more? Sorting through a deceased's online life for the important things can be just as daunting as cleaning out the house of a hoarder.

To make matters worse, the rights of executors, agents, guardians, and beneficiaries with regard to digital assets are unclear as discussed later in this article. Thus, family members may have to go to court for legal authority to gain access to these accounts. Even after gaining legal authority, the company running the online account still may not acquiesce to a family member's authority without a battle.

This process is complicated further if someone is incapacitated rather than deceased because that person will continue to have expenses that a deceased person would not have. Without passwords, a power of attorney alone may not be enough for the agent to pay these expenses. If no power of attorney is in place, a guardian may have to be appointed to access these accounts, and some companies will still require a specific court order on top of that before they release account information.

B. To Prevent Identity Theft

In addition to needing access to online accounts for personal reasons and closing probate, family members need this information quickly so that a deceased's identity is not stolen. Until authorities update their databases regarding a new death, criminals can open credit cards, apply for jobs under a dead person's name, and get state identification cards. There are methods of protecting a deceased's identity, but they all involve having access to the deceased's online accounts. See Aleksandra Todorova, [Dead Ringers: Grave Robbers Turn to ID Theft](#), WALL ST. J., Aug 4, 2009.

C. To Prevent Financial Losses to the Estate

1. Bill Payment

Electronic bills for utilities, loans, insurance, and other expenses need to be discovered quickly and paid to prevent cancellations. This concern is augmented further if the deceased or incapacitated ran an online business and is the only person with access to incoming orders, the servers, corporate bank accounts, and employee payroll accounts. See Tamara Schweitzer, [Passing on Your Digital Data](#), INC., Mar. 1, 2010. Bids for items advertised on eBay may go unanswered and lost forever.

2. Domain Names

The decedent may have registered one or more domain names that have commercial value. If registration of these domain names is not kept current, they can easily be lost to someone waiting to snag the name upon a lapsed registration.

Here is list of some of the most expensive domain names that have been sold in recent years:

1. VacationRentals.com for \$35 million
2. Insure.com: 2009 for \$16 million
3. Sex.com: 2010 for \$14 million
4. Fund.com: 2008 for £9.99 million
5. Porn.com: 2007 for \$9.5 million
6. Fb.com: 2010 for \$8.5 million
7. Business.com: 1999 for \$7.5 million
8. Diamond.com: 2006 for \$7.5 million

9. Beer.com: 2004 for \$7 million
10. Israel.com: 2008 for \$5.88 million
11. Casino.com: 2003 for \$5.5 million
12. Slots.com: 2010 for \$5.5 million
13. Toys.com: 2009 for \$5.1 million
14. Asseenontv.com: 2000 for \$5.1 million
15. iCloud.com: 2011 for \$4.5 million
16. GiftCard.com: 2012 for \$4 million
17. AltaVista.com: 1998 for \$3.3 million
18. Candy.com: 2009 for \$3.0 million
19. Loans.com: 2000 for \$3.0 million
20. Gambling.com: 2011 for \$2.5 million

[List of most expensive domain names](#), Wikipedia (updated Aug. 16, 2013).

3. Encrypted Files

Some digital assets of value may be lost if they cannot be decrypted. Consider the case of Leonard Bernstein who died in 1990 leaving the manuscript for his memoir entitled *Blue Ink* on his computer in a password-protected file. To this day, no one has been able to break the password and access what may be a very interesting and valuable document. See Helen W. Gunnarsson, *Plan for Administering Your Digital Estate*, 99 ILL. B.J. 71 (2011).

4. Virtual Property

The decedent may have accumulated valuable virtual property for use in on-line games. For example, a planet for the *Entropia Universe* sold for \$6 million in 2011 and a space station for the same game sold for \$635,000 in 2010. Andrea Divirgilio, [Most Expensive Virtual Real Estate Sales](#), Bornrich.com (Apr. 23, 2011) (also discussing other high priced sales of virtual property); Oliver Chiang, [Meet The Man Who Just Made a Half Million From the Sale of Virtual Property](#), Forbes.com (Nov. 13, 2010). There are also reports of more “reasonable” prices for virtual items such as a virtual sword for use in *Age of Wulin*, a video game, which was sold for \$16,000. Katy Steinmetz, [Your Digital Legacy: States Grapple with Protecting Our Data After We Die](#), Time Tech (Nov. 29, 2012).

D. To Avoid Losing the Deceased’s Personal Story

Many digital assets are not inherently valuable, but are valuable to family members who extract meaning from what the deceased leaves behind. Historically, people kept special pictures, letters, and journals in shoeboxes or albums for future heirs. Today, this material is stored on computers or online and is often never printed. Personal blogs and Twitter feeds have replaced physical diaries, and e-mails have replaced letters. Without alerting family members that these assets exist, and without telling them how to get access to them, the story of the life of the deceased may be lost forever. This is not only a tragedy for family members, but also possibly for future historians who are losing pieces of history in the digital abyss. Rob Walker, [Cyberspace When You’re Dead](#), N.Y. TIMES, Jan. 5, 2011.

For more active online lives, this concern may also involve preventing spam from infiltrating a loved one’s website or blog site. Comments from friends and family are normally welcomed, but it is jarring to discover the comment thread gradually infiltrated with links for “cheap Ugg boots.” *Id.* “It’s like finding a flier for a dry cleaner stuck among flowers on a grave, except that it is much harder to remove.” *Id.* In the alternative, family members may decide to delete the deceased’s website against the deceased’s wishes simply because those wishes were not expressed to the family.

E. To Prevent Unwanted Secrets from Being Discovered

Sometimes people do not want their loved ones discovering private emails, documents, or other electronic material. They may contain hurtful secrets, non politically correct jokes and stories, or personal rantings. The decedent may have a collection of adult recreational material (porn) which he or she would not want others to know had been accumulated. A professional such as an attorney or physician may have files containing confidential client information. Without designating appropriate people to take care of electronically stored materials, the wrong person may come across this type of information and use it in an inappropriate or embarrassing manner.

F. To Prepare for an Increasingly Information-Drenched Culture

Although the principal concern today appears to be the disposition of social media and e-mail contents, the importance of planning for digital assets will increase each day. Online information will continue to spread out across a growing array of flash drives, iPhones, and iPads, and it will be more difficult to locate and accumulate. As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important. If a foundation for planning for these assets isn't set today, we may re-learn the lesson the Rosetta Stone once taught us: "there is no present tense that can long survive the fall and rise of languages and modes of recordkeeping." Ken Strutin, [*What Happens to Your Digital Life When You Die?*](#), N.Y. L.J., Jan. 27, 2011 (For fifteen centuries, the meaning of the hieroglyphs on the Rosetta Stone detailing the accomplishments of Ptolemy V were lost when society neglected to safeguard the path to deciphering the writings. A Napoleonic soldier eventually discovered the triptych, enabling society to recover its writings.).

IV. USER AGREEMENTS

A. Terms of Service

When an individual signs up for a new online account or service, the process typically requires an agreement to the provider's terms of service. Service providers may have policies on what will happen on the death of an account holder but individuals rarely read the terms of service carefully, if at all. Nonetheless, the user is at least theoretically made aware of these policies before being able to access any service. Anyone who has signed up for an online service has probably clicked on a box next to an "I agree" statement near the bottom of a web page or pop-up window signifying consent to the provider's terms of use. The terms of these "clickwrap" agreements are typically upheld by the courts.

For example, Google's terms of service do not include an explicit discussion of what happens when the account holder dies. The terms state that the individual agrees not to "assign (or grant a sub-

license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software," although copyright remains in the user. [*Google Terms of Service*](#), GOOGLE APPS, #7 (last visited Sept. 4, 2013). In a somewhat comical provision that seems to envision Google's concern of a user coming back as a vampire or zombie, the terms provide that "upon receipt of a certificate or other legal document confirming your death, Google will close your account and you will no longer be able to retrieve content contained in that account."

Google's e-mail service, Gmail, on the other hand, does have its own policy, explained in its help section, for "Accessing a Deceased Person's Mail." Here are some of the key provisions of the policy:

If you need access to the Gmail account content of an individual who has passed away, in rare cases we may be able to provide the contents of the Gmail account to an authorized representative of the deceased person.

At Google, we're keenly aware of the trust users place in us, and we take our responsibility to protect the privacy of people who use Google services very seriously. Any decision to provide the contents of a deceased person's email will be made only after a careful review.

Before you begin, please understand that Google may be unable to provide the Gmail account content, and sending a request or filing the required documentation does not guarantee that we will be able to assist you. The application to obtain email content is a lengthy process with multiple waiting periods. If you are the authorized representative of a deceased person and wish to proceed with an application to obtain the contents of a deceased person's Gmail account, please carefully review the following information regarding our two stage process.

[*Accessing a Deceased Person's Mail*](#), GMAIL HELP, (last visited Sept. 4, 2013).

At the end of its terms of service, Yahoo! explicitly states that an account cannot be

transferred: “You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.” *Yahoo! Terms of Service*, Yahoo! (last visited Sept. 4, 2013).

Facebook, the world’s most popular online social network, recognized a need to allow a deceased person’s wall to provide a source of comfort in 2009. See Jess Moore, *Facebook Memorials a Part of Campus Life*, USA TODAY (Mar. 22, 2011); Matthew Moore, *Facebook Introduces ‘Memorial’ Pages to Prevent Alerts About Dead Members*, THE TELEGRAPH (Oct. 27, 2009); *Facebook, Inc.*, The New York Times (Oct. 5, 2012). It permits someone to “Report a Deceased Person’s Profile.” *How Do I Report a Deceased User or an Account That Needs to be Memorialized or Deleted?*, Facebook Help Center?, *Memorialization Request* (last visited Sept. 4, 2013). When Facebook receives proof of death through an obituary or a news article, the page can be “memorialized,” so that only confirmed friends will continue to have access. Because the “wall” remains, friends can still post on the memorialized page. (Facebook “walls” are an interactive feature of a user’s “profile” page which reflect the user’s recent Facebook activity. Depending on user privacy settings, the wall enables a view of recent status updates, changes to the user’s profile information, photos posted by or of the user, sharing links and other Internet content, and interactive comments regarding all such content between the user and his or her Facebook “friends.” See John Miller, *Is MySpace Really My Space?: Examining the Discoverability of the Content of Social Media Accounts*, 30 No. 2 Trial Advoc. Q. 28, 29 (2011).).

B. Ownership

A problem may also arise if the client does not actually own the digital asset but merely has a license to use that asset while alive. It is unlikely a person can transfer to heirs or beneficiaries music, movies, and books they have purchased in electronic form although they may transfer “old school” physical records (vinyl), CDs, DVDs,

books, etc. without difficulty. It has been reported that actor Bruce Willis wants to leave his large iTunes music collection to his children but that Apple’s user agreement prohibits him from doing so. See Brandon Griggs, *Can Bruce Willis Leave His iTunes Music to His Kids?*, CNN.com (Sept. 4, 2012). See also Roger Yu, *Digital Inheritance Laws Remain Murky*, USA TODAY, Sept. 19, 2012; See Aileen Entwistle, *Safeguarding Your Online Legacy After You’ve Gone*, Scotsman. Com, March 30, 2013 (iTunes and Kindle books are only lifetime licenses).

V. FEDERAL LAW

Federal law regulates the unauthorized access to digital assets and addresses the privacy of online communication. See Deven R. Desai, *Property, Persona, and Preservation*, 81 TEMP. L. REV. 67 (2008); Molly Wilkens, *Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?*, 62 HASTINGS L.J. 1037 (2011); Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Allan D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295 (2012).

While the statutes themselves do not directly address issues involving fiduciary’s access to digital assets and accounts, they can create constraints for individuals attempting to plan for their digital assets and their fiduciaries.

A. Stored Communications Act

The Stored Communications Act, 18 USC § 2701(a), makes it a crime for a person to “intentionally access[] without authorization a facility through which an electronic communication service is provided.” It also criminalizes the intentional exceeding of access to the facility. The Act, however, does not apply to conduct which is authorized by the user.

Section 2702 prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service, unless disclosure is

made “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.”

B. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 also prohibits the unauthorized access to computers.

C. Interface With User Agreements

Problems may arise if the terms of service prohibit a user from granting others access to the account. If a user reveals his or her user name and password and another person uses that information to access an account, it could be in violation of these acts as being without “lawful consent.”

One approach being taken by some states, which either have or are considering granting personal representatives the ability to access the accounts, is to provide by statute that such access is not a breach of any terms of the user agreement. For example, the proposed Nevada statute states:

The act by a personal representative to take control of, conduct or continue any account or asset of a decedent * * * does not invalidate or abrogate any conditions, terms of service or contractual obligations the holder of such an account or asset has with the provider or administrator of the account, asset or Internet website.

[Nev. Senate Bill 131](#) (as amended Apr. 17, 2013).

As another example, the proposed Virginia statute provides:

This section supersedes any contrary provision in the terms of service agreement, and a fiduciary shall be considered an authorized user who has the lawful consent of the person or estate to whom he owes a fiduciary duty for purposes of accessing or possessing such person's or estate's digital accounts and digital assets.

Virginia [S.B. 914](#), 2013 Session.

Many issues may arise, however, with this type of provision.

- Do such statutory provisions interfere with freedom of contract and/or already established contract rights?
- Will contrary provisions in the terms of service agreement be deemed unenforceable as against public policy?
- How will choice of law provisions in the user agreements which indicate that the agreement is governed by the law of some other state or country be handled?
- Are statutes which attempt to circumvent the federal statutes unconstitutional?

VI. PLANNING SUGGESTIONS

Legal uncertainty reinforces the importance of planning to increase the likelihood that an individual's wishes concerning the disposition of digital assets will be actually carried out. Even individuals with digital property are not taking steps to plan for that property. *See* Becky Yerak, [Online Accounts After Death: Remember Digital Property When Listing Assets](#), CHICAGO TRIB., Aug. 26, 2012. (reporting that a survey by BMO Retirement Institute revealed that 57% of respondents who believed it was very or somewhat important to plan for digital assets had not made such plans).

Currently, many attorneys do not include such planning as part of their standard set of services, however, they should begin to do so immediately. *See* Kelly Greene, [Passing Down Digital Assets](#), WALL ST. J., Aug. 31, 2012. Digital assets are valuable, both emotionally and financially, and they are pervasive.

A. Specify Disposition According to Provider's Instructions

Though most Internet service providers have a policy on what happens to the accounts of deceased users, these policies are not prominently posted and many users may not be aware of them. If they are part of the standard terms of service, they may not appear on the initial screens as users quickly click through them.

In April 2013, Google took an innovative first step by creating the [*Inactive Account Manager*](#) which users may use to control what happens to emails, photos, and other documents stored on Google sites such as +1s, Blogger, Contacts and Circles, Drive, Gmail, Google+ Profiles, Pages and Streams, Picasa Web Albums, Google Voice, and YouTube. The user sets a period of time after which the user's account is deemed inactive. Once the period of time runs, Google will notify the individuals the user specified and, if the user so indicated, share data with these users. Alternatively, the user can request that Google delete all contents of the account. See [*About Inactive Account Manager*](#), Google (last visited Apr. 3, 2015).

In February 2015, Facebook began allowing its users to name a "legacy contact" to manage certain parts of their accounts after they die. Users may also opt to have their material completely deleted. See Facebook, [*What is a Legacy Contact*](#), (last visited Apr. 3, 2015).

B. Back-Up to Tangible Media

The user should consider making copies of materials stored on Internet sites or "inside" of devices on to tangible media of some type such as a CD, DVD, portable hard drive, or flash drive. The user can store these materials in a safe place, such as a safe deposit box, and then leave them directly to named beneficiaries in the user's will. Of course, this plan requires constant updating and may remove a level of security if the files on these media are unencrypted. However, for some files such as many years of vacation and family photos, this technique may be effective.

C. Prepare Comprehensive Inventory of Digital Estate

1. Creation

An initial estate planning questionnaire should include questions about the client's digital assets. While people may think of bank accounts, stock accounts, real estate, and other brick-and-mortar items as property suitable for estate planning, they may not have considered their digital assets. Accordingly, an attorney can help. In this situation, individuals need to develop an inventory of these assets, including a list of how

and where they are held, along with usernames, passwords, and answers to "secret" questions. A sample form is included in the Appendix to this article. Lawyers can then provide advice on what happens in the absence of planning, the default system of patchwork laws and patchy Internet service provider policies, as well as the choices for opting out of the default systems.

2. Storage

Careful storage of the inventory document is essential. Giving a family member or friend this information while alive and well can backfire on your clients. For example, if a client gives his daughter his online banking information to pay his bills while he is sick, siblings may accuse her of misusing the funds. Further, a dishonest family member would be able to steal your client's money undetected.

If you decide that a separate document with digital asset information is the best route for your client, this document should be kept with your client's will and durable power of attorney in a safe place. The document can be delivered to the client's executor upon the client's death or agent upon the client's incapacity. You may consider encrypting this document and keeping the passcode in a separate location as a further safeguard.

Another option is to use an online password storage service such as 1Password, KeePass, or my-iWallet. Your client would then need to pass along only one password to a personal representative or agent. See Nancy Anderson, [*You Just Locked Out Your Executor and Made Your Estate Planning a Monumental Hassle*](#), FORBES, Oct. 18, 2012. However, this makes this one password extremely powerful as now just one "key" unlocks the door to your client's entire digital world.

Warning: Giving someone else the client's user name and password may be against the terms of service in the contract. Accordingly, if someone uses your client's access information, it may be deemed a state or federal crime because it exceeds the access to that information that is stated in the user agreement.

D. Provide Immediate Access to Digital Assets

Your client may be willing to provide family members and friends immediate access to some digital assets while still alive. Your client may store family photographs and videos on websites such as Shutterfly and DropShots, which permit multiple individuals to have access. Your client could create a YouTube channel. See Nancy Anderson, [*You Just Locked Out Your Executor and Made Your Estate Planning a Monumental Hassle*](#), FORBES, Oct. 18, 2012.

E. Authorize Agent to Access Digital Assets

The client may include express directions in a durable power of attorney authorizing the agent to access his or her digital accounts. However, as mentioned above, it is uncertain whether the agent can use that authority in a legal manner to access the information depending on the terms of service agreement.

Below is a provision adapted from a clause suggested by Keith P. Huffman, [*Law Tips: Estate Planning for Digital Assets*](#), Indiana Continuing Legal Education Forum (Dec. 4, 2012):

Digital Assets. My agent has (i) the power to access, use, and control my digital device, including, but not limited to, desktops, laptops, peripherals, storage devices, mobile telephones, smart phones, and any similar device which currently exists or exists in the future as technology develops for the purpose of accessing, modifying, deleting, controlling or transferring my digital assets, and (ii) the power to access, modify, delete, control, and transfer my digital assets, including, but not limited to, any emails, email accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, domain registrations, web hosting accounts, tax preparation service accounts, on-line stores, affiliate programs, other on line programs, including frequent flyer and other bonus programs, and similar digital items which currently exist or exist in the future as technology develops.

F. Place Digital Assets in a Trust

One of the most innovative solutions for dealing with digital assets is to create a revocable trust to hold the assets. See Joseph M. Mentrek, *Estate Planning in a Digital World*, 19 Ohio Prob. L.J. 195 (May/June 2009). A trust may be a more desirable place for account information than a will because it would not become part of the public record and is easier to amend than a will.

The owner could transfer digital property into a trust and provide the trustee with detailed instructions regarding management and disposition. Assuming the asset is transferable, the digital asset could be folded into an existing trust. See Jessica Bozarth, *Copyrights & Creditors: What Will Be Left of the King of Pop's Legacy?*, 29 CARDOZO ARTS & ENT. L.J. 85, 104-07 (2011). An individual also could set up a separate trust just to hold digital property or to hold specified digital assets. However, creating a separate revocable trust for digital assets may be overkill for many individuals and only be practical for those with digital assets of substantial value.

The client could register accounts in the name of the trust so the successor trustee would legally (and, one hopes, seamlessly) succeed to these accounts. In addition, many digital assets take the form of licenses that expire upon death. They may survive the death of the settlor if the trust owns these accounts and assets instead.

When a person accumulates more digital assets, designating these assets as trust assets may be as simple as adding the word "trustee" after the owner's last name. See John Conner, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death*, 4 EST. PLAN. & COMM. PROP. L.J. 301 (2011).

G. Place Digital Asset Information in a Will

When determining how to dispose of digital assets, one's first instinct may be to put this information in a will. However, a will may not be the best place for this information for several reasons. Because a will becomes public record once admitted to probate, placing security codes and passwords within it is dangerous. Further, amending a will each time a testator changes a password would be cumbersome and expensive.

If a client actually wishes to pass on a digital asset rather than the information of how to deal with the asset, a will may not be the proper transfer mechanism.

A will, however, is useful for limited purposes. For example, your client could specify beneficiaries of specific digital assets especially if those assets are of significant monetary value. A testator may also reference a separate document such as the inventory discussed above that contains detailed account information which would provide the executor with invaluable information.

If the ownership of the digital asset upon death is governed by the user agreement, the asset may actually be of the non-probate variety. Thus, like a multiple-party bank account or life insurance policy, the digital asset may pass outside of the probate process.

Because only a few states have statutes authorizing a personal representative to gain access to digital assets, it may be prudent to include a provision granting such authority in wills. The following provision is suggested by James Lamm. See Michael Froomkin, [*Estate Planning for Your Digital Afterlife*](#), Discourse.net (Feb. 18, 2013).

The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information. 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 the personal representative: (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; (3) any record or other information pertaining to me with respect to that service. 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. The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private.

H. Use Online Afterlife Company

Recently, entrepreneurs recognizing the need for digital estate planning have created companies that offer services to assist in planning for digital assets. These companies offer a variety of services to assist clients in storing information about digital assets as well as notes and emails that clients wish to send post-mortem. As an estate planning attorney, you may find this additional service to be valuable and recommend one to your clients.

A non-exclusive list of the different companies and the services they offer is set forth below in

alphabetical order. The author is not recommending any of these companies and no endorsement should be implied because of a company's inclusion or exclusion from this list. You must use due diligence in investigating and selecting a digital afterlife company. For example, in the two years I have been maintaining this list, about one-third of the companies have gone out of business or merged with another similar firm.

Name	Services Offered
AfterSteps	Provides users with a step-by-step guide in planning their estate, financial, funeral, and legacy plans, which will be transferred to the users' designated beneficiaries upon passing.
AssetLock	Enables users to upload documents, final letters, final wishes, instructions, important locations, and secret information to an online safe deposit box. Once the user dies and a minimum number of recipients confirm the user's death, AssetLock will release pre-designated information to the pre-designated recipients.
Cirrus Legacy	Enables users to keep track of their email accounts, online banking, PayPal, ebay, Amazon, and web hosting, and how these will be passed on.
Dead Man's Switch	Enables users to write emails and designate recipients. Once user fails to respond to three emails, Dead Man's Switch releases the emails to the recipients.
DeadSocial	Sends messages after death via Facebook and Twitter.
Deathswitch	Enables users to write emails and designate recipients.
Estate Map	Moves an estate planning attorney's intake and enables clients to securely store and pass on important estate information.
Estate++	Enables users to upload important legal documents, photographs, notes, and instructions to a virtual safe deposit box.
E-Z-Safe	Enables users to securely store, update, retrieve, and pass their growing digital assets.
If I Die	Enables users to write notes that will be sent to pre-designated recipients at death.

Name	Services Offered
Legacy Locker	Enables users to save all online account information in a digital safe deposit box and assign beneficiaries for each account.
LivesOn	Allows a person to "continue" tweeting after death and to name a person with authority to continue the account.
My Wonderful Life	Enables users to leave letters, instructions, information, and photographs for pre-designated recipients.
Parting Wishes	Enables users to draft online estate planning documents, design online memorials, create web pages about their lives, prepare final messages, document funeral wishes, and designate Keyholders to distribute this information.
Secured Safe [formerly DataInherit, Entrustet, and others]	Provides users with online storage for passwords and digital documents.
SlightlyMorbid	Enables users to leave behind emails, instructions, and personal online contacts.
Vital Lock	Posthumously delivers text, videos, images, audio recordings, and links to pre-designated recipients.

VII. OBSTACLES TO PLANNING FOR DIGITAL ASSETS

Including digital assets in estate plans is a new phenomenon. Many of the kinks have not yet been straightened out. Some of the problem areas include safety issues involved with passwords, the hassle of updating this information, the uncertainty surrounding online afterlife management companies, and the fact that some online afterlife management companies overstate their abilities.

A. Safety Concerns

Clients may be hesitant to place all of their usernames, passwords, and other information in one place. We have all been warned, "Never write down your passwords." This document could fall into the hands of the wrong person, leaving your client exposed. One option to safeguard against this is to have your clients create two documents; one with usernames and

one with passwords. The documents can be stored in different locations or given to different individuals. With an online afterlife management company or an online password vault, clients may worry that the security system could be breached, leaving them completely exposed. *See* Deborah L. Jacobs, [*Six Ways to Store Securely the Keys to Your Online Financial Life*](#), FORBES, Feb. 15, 2011. The same concern is present if your client chooses to place all this information in one document.

B. Hassle

Planning for digital assets is an unwanted burden. Digital asset information is constantly changing and may be stored on a variety of devices (e.g., desktop computers, laptop computers, smart phones, cameras, iPads, CDs, DVDs, and flashdrives). A client may routinely open new email accounts, new social networking or gaming accounts, or change passwords. Documents with this information must be revised and accounts at online afterlife management companies must be frequently updated. For clients who wish to keep this information in a document, advise them to update the document quarterly and save it to a USB flash drive or in the cloud, making sure that a family member, friend, or attorney knows where to locate it. *See* Tamara Schweitzer, [*Passing on Your Digital Data*](#), INC., Mar. 1, 2010.

C. Uncertain Reliability of Online Afterlife Management Companies

Afterlife management companies come and go; their life is dependent upon the whims and attention spans of their creators and creditors. Lack of sustained existence of all of these companies make it hard, if not impossible, to determine whether this market will remain viable. Clients may not want to spend money to save digital asset information when they are unsure about the reliability of the companies. *See id.*

D. Overstatement of the Abilities of Online Afterlife Management Companies

Some of these companies claim they can distribute digital assets to beneficiaries upon your client's death. Explain to your clients that these companies cannot do this legally, and that they

need a will to transfer assets, no matter what kind. Using these companies to store information to make the probate process easier is fine but they cannot be used to avoid probate altogether. David Shulman, an estate planner in Florida, stated that he "would relish the opportunity to represent the surviving spouse of a decedent whose eBay business was 'given away' by Legacy Locker to an online friend in Timbuktu." David Shulman, [*Estate Planning for Your Digital Life, or, Why Legacy Locker Is a Big Fat Lawsuit Waiting to Happen*](#), SOUTH FLORIDA ESTATE PLANNING LAW (Mar. 21, 2009).

E. Federal Law Restrictions

There are at least two unresolved issues raised by Federal law. The first is whether the fiduciary is "authorized" to access the digital property pursuant to the statutes prohibiting unauthorized access to computers and computer data. *See* Jim Lamm, [*Facebook Blocks Demand for Contents of Deceased User's Account*](#), Oct. 11, 2012, (discussing [*In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things*](#), the Daftary case, in which the court held that the Stored Communications Act's privacy rights protect Facebook contents and that Facebook cannot be compelled to turn over the contents).

A second issue is whether the fiduciary can request that the provider disclose records. In that situation, the fiduciary does not go online but rather asks the provider for the records. The critical question here is determining that the fiduciary becomes the subscriber for purposes of permitting access under one of the exceptions to the Stored Communications Act. While state law can clarify that the fiduciary is an authorized user, this is an issue of federal law.

The problem of fiduciary access possibly being in violation of the law is also an issue in other nations such as the United Kingdom where using a deceased's username and password could result in the person who gains access violating the Computer Misuse Act of 1990. *See* Aileen Entwistle, [*Safeguarding Your Online Legacy After You've Gone*](#), Scotsman. Com, March 30, 2013.

VIII. FIDUCIARY ACCESS TO DIGITAL ESTATE

The rights of executors, administrators, agents, and guardians with regard to digital assets are muddy. Their rights in the digital world can be analogized to their rights in the brick-and-mortar world, for which there are well-established probate laws governing access, as well as established procedures designed to safeguard the power of attorney process. *See, e.g.*, UNIFORM POWER OF ATTORNEY ACT (2008); Kathryn T. McCarty & Mark R. Singler, *Practical Estate Planning for the Elder Client*, 24-Mar CBA Rec. 30, 31-32 (2010). However, the practical extension of these laws to digital assets is just beginning to be tested.

A. Existing State Law

Existing legislation takes a variety of forms, and can be divided into different “generations.” Each generation is a group of statutes covering similar (or identical) types of digital assets, often under an analogous access structure. The first generation, comprising California, Connecticut, and Rhode Island, only cover e-mail accounts. Perhaps recognizing the shortcomings of such a limited definition, Indiana’s second-generation statute, enacted in 2007, is more open-ended, covering records “stored electronically.” The third generation statutes, enacted since 2010 in Oklahoma, Idaho, Nevada, and Louisiana explicitly expand the definition of digital assets to include social media and microblogging (e.g., Twitter). States that enact either a version of the Uniform Fiduciary Access to Digital Assets Act (UFADAA or RUFADAA) or the Privacy Expectation Afterlife and Choices Act (PEAC) comprise the fourth generation.

As of this writing, Delaware is the only state to enact a statute “close enough” to UFADAA so that NCCUSL considers the legislation to be a UFADAA adoption although it has been introduced in twenty-six other states. As of May 22, 2016, 13 states have enacted RUFADAA and it is pending in 18 other states.

Virginia is the only state to enact PEAC and it remains pending in a few states.

Note that these generations are not necessarily distinct in time as legislation of each generational

type has recently been proposed in various states. *See generally* Jason Mazzone, *Facebook’s Afterlife*, 90 N. CAR. L. REV. 1643 (2012).

1. First Generation

The first generation statutes, enacted as early as 2002, only cover e-mail accounts. They do not contain provisions enabling or permitting access to any other type of digital asset.

a. California

The first and most primitive first generation statute was enacted by California in 2002. This statute is not specifically directed to personal representatives and simply provides, “Unless otherwise permitted by law or contract, any provider of electronic mail service shall provide each customer with notice at least 30 days before permanently terminating the customer’s electronic mail address.” [CAL. BUS. & PROF. CODE § 17538.35](#) (West 2010). Providers are likely to provide this notice via e-mail. *See* Jonathan J. Darrow & Gerald R. Ferrera, *Who Owns a Decedent’s E-Mails: Inheritable Probate Assets or Property of the Network?*, 10 N.Y.U. J. Legis. & Pub. Pol’y, 281, 296 (2006-2007). Consequently, in the case of a deceased account holder, the notice will be “wholly useless” unless the personal representative has rapid access to the decedent’s e-mail account and monitors it regularly. Tyler G. Tarney, *A Call for Legislation to Permit the Transfer of Digital Assets at Death*, 40 Cap. U. L. Rev. 773, 788 (2012).

b. Connecticut

Connecticut was one of the first states to address executors’ rights to digital assets. In 2005, the legislature passed S.B. 262, requiring “electronic mail providers” to allow executors and administrators “access to or copies of the contents of the electronic mail account” of the deceased, upon showing of the death certificate and a certified copy of the certificate of appointment as executor or administrator, or by court order. S.B. 262, 2005 Leg., Reg. Sess. (Conn. 2005) (codified at [CONN. GEN. STAT. ANN. § 45a-334a](#) (West 2012)). The bill specifically defined “electronic mail service providers” as “sending or receiving electronic mail” on behalf of end-users. *Id.*

RUFADAA is pending as of May 22, 2016.

c. Rhode Island

In 2007, Rhode Island passed the Access to Decedents' Electronic Mail Accounts Act, requiring "electronic mail service providers" to provide executors and administrators "access to or copies of the contents of the electronic mail account" of the deceased, upon showing of the death certificate and certificate of appointment as executor or administrator, or by court order. H.B. 5647, 2007 Leg., Jan. Sess. (R.I. 2007) (codified at [R.I. GEN. LAWS § 33-27-3](#) (2012)). Rhode Island uses a definition of "electronic mail service provider" similar to Connecticut's: "an intermediary in sending or receiving electronic mail" who "provides to end-users . . . the ability to send or receive electronic mail." *Id.*

RUFADAA is pending as of May 22, 2016.

2. Second Generation (Indiana)

Perhaps in acknowledgement of changing technological times, one state has a second generation statute which uses a broad definition of covered digital assets. While an open-ended definition may allow the law to remain relevant as new technologies are invented and new types of digital assets gain prominence, its generality may also create confusion and uncertainty as to what assets will actually be covered and how best to engage in planning for them.

In 2007, the Indiana legislature added a provision to its state code requiring custodians of records "stored electronically" regarding or for an Indiana-domiciled decedent, to release such records upon request to the personal decedent's personal representative. [IND. CODE § 29-1-13-1.1 \(2007\)](#). The personal representative must furnish the custodian either (1) a copy of the death certificate and letters testamentary or (2) a court order. *Id.* After the custodian is notified of the decedent's death, the custodian may not dispose of or destroy the electronic records for two years. Custodians need not release records "in violation of any applicable federal law" or "to which the deceased person would not have been permitted in the ordinary course of business." *Id.*

RUFADAA takes effect in Indiana on July 1, 2016.

3. Third Generation

Third generation legislation acknowledges the changes to the digital asset landscape, since California enacted its first generation e-mail legislation in 2002. These third generation laws expressly recognize new and popular digital assets – social networking and microblogging. While these laws may better serve the current population than the limited first generation statutes, they share the same risk of becoming obsolete in only a few years.

a. Oklahoma

In 2010, Oklahoma enacted legislation with a fairly broad scope, giving executors and administrators "the power . . . 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 e-mail service websites." H.B. 2800, 52nd Leg., 1st Sess. (Okla. 2010) (codified at [OKLA. STAT. tit. 58, § 269](#) (2012)).

RUFADAA is pending as of May 22, 2016.

b. Idaho

On March 26, 2012, Idaho amended its Uniform Probate Code to enable personal representatives and conservators to "[t]ake control of, conduct, continue or terminate any accounts of the decedent on any social networking website, any microblogging or short message service website or any e-mail service website." [S.B. 1044, 61st Leg., Reg. Sess.](#) (Idaho 2011). Sponsors declared that the purpose of the bill was to "make it clear" that personal representatives and conservators can control the decedent's or protected person's "social media . . . such as e-mail, blogs instant messaging, Facebook types of accounts, and so forth." Statement of Purpose, 1044-RS20153, Leg. 61, Reg. Sess. (Idaho 2011).

Idaho adopted RUFADAA in 2016.

c. Nevada

Effective October 1, 2013, Nevada authorizes a personal representative to direct the termination of, but not access to, e-mail, social networking, and similar accounts. [Nev. 2013 Sess. Laws ch. 325](#).

In an attempt to avoid problems with federal law, the statute states:

The act by a personal representative to direct the termination of any account or asset of a decedent *** does not invalidate or abrogate any conditions, terms of service or contractual obligations the holder of such an account or asset has with the provider or administrator of the account, asset or Internet website.

d. Louisiana

In 2014, Louisiana granted succession representatives the right to obtain access or possession of a decedent's digital accounts within thirty days after receipt of letters. The statute attempts to trump contrary provisions of service agreements by deeming the succession representative to be an authorized user who has the decedent's lawful consent to access and possess the accounts. [La. Rev. Stat. § 3191](#).

RUFADAA is pending as of May 22, 2016.

4. Specialized State Legislation (Virginia)

In 2013, Virginia enacted [§ 64.2-110](#) which grants the personal representative of a deceased minor access to the minor's digital accounts such as those containing e-mail, social networking information, and blogs. The personal representative assumes the deceased minor's terms of service agreement for the purposes of consenting to and obtaining the disclosure of the contents of the account.

The reason this legislation is limited to minors is because its chief proponent, Ricky Rash, wants to obtain information from his son's Facebook account which he hopes will explain why his son committed suicide. See Evan Carroll, [Virginia Passes Digital Assets Law](#), The Digital Beyond, Feb. 19, 2013.

B. Uniform Fiduciary Access to Digital Assets Act

1. Overview and Supporting Arguments

The National Conference of Commissioners on Uniform State Laws approved the [Uniform Fiduciary Access to Digital Assets Act](#)

(UFADAA) on July 29, 2014. Below is an excerpt from the Conference's summary of UFADAA:

UFADAA gives people the power to plan for the management and disposition of their digital assets in the same way they can make plans for their tangible property: by providing instructions in a will, trust, or power of attorney. If a person fails to plan, the same court-appointed fiduciary that manages the person's tangible assets can manage the person's digital assets, distributing those assets to heirs or disposing of them as appropriate.

Some custodians of digital assets provide an online planning option by which account holders can choose to delete or preserve their digital assets after some period of inactivity. UFADAA defers to the account holder's choice in such circumstances, but overrides any provision in a click-through terms-of-service agreement that conflicts with the account holder's express instructions.

Under UFADAA, fiduciaries that manage an account holder's digital assets have the same right to access those assets as the account holder, but only for the limited purpose of carrying out their fiduciary duties. Thus, for example, an executor may access a decedent's email account in order to make an inventory of estate assets and ultimately to close the account in an orderly manner, but may not publish the decedent's confidential communications or impersonate the decedent by sending email from the account. Moreover, a fiduciary's management of digital assets may be limited by other law. For example, a fiduciary may not copy or distribute digital files in violation of copyright law, and may not access the contents of communications protected by federal privacy laws.

In order to gain access to digital assets, UFADAA requires a fiduciary to send a request to the custodian, accompanied by a certified copy of the document granting fiduciary authority, such as a letter of appointment, court order, or certification

of trust. Custodians of digital assets that receive an apparently valid request for access are immune from any liability for good faith compliance.

UFADAA is an overlay statute designed to work in conjunction with a state's existing laws on probate, guardianship, trusts, and powers of attorney. Enacting UFADAA will simply extend a fiduciary's existing authority over a person's tangible assets to include the person's digital assets, with the same fiduciary duties to act for the benefit of the represented person or estate. It is a vital statute for the digital age, and should be enacted by every state legislature as soon as possible.

As of this writing, Delaware is the only state to enact a statute "close enough" to UFADAA so that [NCCUSL considers the legislation to be an UFADAA enactment](#). [50 Del Code §§ 5001-5007](#).

UFADAA was introduced but was not enacted in Colorado, Maryland, Mississippi, North Dakota, Texas, Virginia, Washington, and Wyoming. At the time of this writing,

See also Victoria Blachly, *Uniform Fiduciary Access to Digital Assets Act*, PROB. & PROP., July/Aug. 2015, at 8.

2. Opposition

Despite the potential benefits of UFADAA, there is significant opposition based on privacy and federal law concerns. On January 12, 2015, four organizations, American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, and Consumer Action, [issued a joint report opposing UFADAA](#) because it provides default access to digital assets. They believe legislation "should instead incentivize individual users to knowingly opt in to the sharing of their electronic communications."

Below are excerpts from their joint letter explaining the reasons for their opposition:

Digital assets are not analogous to physical records.

The ULC model legislation is based on the premise that digital accounts are not fundamentally different than physical

records with respect to estate law. However, given that online accounts are often accessed in private and stored in password-protected formats, it is unlikely that consumers would expect anyone else to have the capacity to access their communications unless they have made a conscious choice to make that information available. Many digital assets differ significantly from physical estates in three important ways:

- Digital accounts often store content by default rather than as an active choice by the individual.
- In many cases there are no storage costs associated with saving digital content for the user, eliminating the burden of storing tremendous volumes of personal data.
- Consumer expectations are as variable as the huge array of digital accounts and cannot be governed by an unconditional rule. * * *

Digital Assets Implicate the Privacy of Third Parties.

The disclosure of digital communications data implicates the privacy not just of the decedent, but of all those who communicated with the deceased, many of whom will still be alive. While the ULC model bill is limited to providing access to fiduciaries of the estate — as opposed to heirs—in practice, a personal representative is likely to be a close family member, especially in the event of an intestate death (more than half of Americans die without a will). * * * Turning over access to communications content compromises the privacy of all those who wrote to the decedent throughout their lives, and gives access to relatives who were never meant to see the communications. Once a representative has access to (and real-time control of) a decedent's accounts, there is no practical limitation on their ability to peruse every single email, IM, or text sent or received by the decedent.

Conservatorships Should Not be Included in Digital Estates Legislation.

One uniquely troubling aspect of UFADAA is its inclusion of conservators among the categories of personal representatives entitled to access an individual's digital accounts. Conservatorships are designed to assist a protected living person with financial or healthcare decisions, and as such implicate delicate questions about disability rights and personal freedom. While a conservatorship may warrant access to a protected person's specific financial or medical accounts—which can currently be accomplished by court order when the circumstances require—it would be a far more acute invasion of privacy to grant unfettered access to all of that individual's online accounts. Even where a conservator is allowed to manage the protected person's social decisions, a grant of access to—and control of—all of that individual's communications on various online platforms (including e-mail, social media, and dating profiles) is completely unwarranted. A presumption that control of a person's digital accounts is a routine aspect of conservatorship significantly impairs a disabled individual's personal autonomy and liberty. * * *

The ULC model legislation conflicts with the federal Electronic Communications Privacy Act.

The Electronic Communications Privacy Act (ECPA) permits providers to voluntarily disclose certain non-content records to anyone other than a governmental entity, but it bars providers from voluntarily disclosing content to anyone except in very limited circumstances. One relevant exception is that providers can voluntarily disclose the contents of a communication with the consent of the author or her "agent." ECPA does not define either "consent" or "agent." Yet the ULC model bill presumes that a fiduciary, without court approval, is entitled to full access to a decedent's estate, without any finding that such fiduciary is also an agent for purposes of federal law. Cloud

service providers interpreting a ULC-based statute and ECPA will be forced to make a legal determination of whether executors or other court-appointed personal representatives are legally "agents" or have the lawful consent of the deceased subscriber. Given that the wrong choice means a potential violation of federal law, the ULC model bill could be wholly ineffective.

C. Privacy Expectation Afterlife and Choices Act

In response to UFADAA, NetChoice, an association of Internet companies that includes Google and Facebook, drafted the [Privacy Expectation Afterlife and Choices Act](#) (PEAC). The PEAC "requires companies to disclose contents only when a court finds that the user is deceased, and that the account in question has been clearly linked to the deceased. Additionally, the request for disclosure must be 'narrowly tailored to effect the purpose of the administration of the estate,' and the executor demonstrates that the information is necessary to resolve the fiscal administration of the estate. And even then, the amount of information is further restricted to the year preceding the date of death. This is stringent guidance meant to protect the privacy of those who communicated with the user while also ensuring that their loved ones can access important financial statements that may be delivered to the account." Alethea Lange, [Everybody Dies: What is Your Digital Legacy?](#), Center for Democracy & Technology (Jan. 23, 2015).

PEAC does not address access by other fiduciaries such as trustees, agents, guardians, and conservators.

As of this writing, Virginia is the only state to have enacted PEAC with some modifications such as extending the time period the information may be requested to 18 months before death rather than one year. Virginia's version of the PEAC took effect on July 1, 2015. [2015 Va. Acts ch. ____ \(SB 1450ER\)](#). PEAC has been introduced in several other states including California and Oregon.

See Karin Prangley, *War and PEAC in Digital Assets*, PROB. & PROP., July/Aug. 2015, at 40.

D. Virginia

As mentioned above, Virginia's version of PEAC took effect on July 1, 2015. Here is a summary of how this new statute operates.

1. Obtaining Deceased User's Records

A personal representative may petition the court to obtain information about the deceased user's records for the 18-month period prior to death such as the names of persons with whom the deceased user communicated, the time and date of the communications, and the electronic addresses of the persons by filing a motion along with an affidavit attesting to the following facts:

- The user is deceased;
- The deceased user was a subscriber of or customer of the provider;
- The account belonging to the deceased user has been reasonably identified;
- There are no other authorized users or, if any, they have consented;
- The request is tailored to effectuate estate administration purposes; and
- The request does not conflict with terms of the deceased user's will.

This request does not authorize the provider to reveal the contents of the communications or the subject lines of the communications.

If the court finds it necessary for the administration of the estate, records beyond the 18-month period may be obtained.

2. Obtaining Contents of Deceased User's Accounts

If the personal representative wishes to obtain the contents of the deceased user's accounts, the personal representative must also demonstrate that the deceased user affirmatively consented to have the contents revealed either by a will provision or a setting within the product or service.

3. Deceased User's Desires Prevail

The court cannot compel a provider to reveal records or their contents if the deceased user affirmatively (1) expressed an intent not to

disclose the records or content of the account through an account setting within the product or service, (2) made an election with a service provider not to disclose the contents of the user's account, or (3) deleted the records or contents during the user's lifetime.

4. Use of Deceased User's Account Prohibited

The court cannot order a provider to allow the personal representative to transmit communications from, post content to, access, or make other use of the deceased user's account.

5. Provider-Orientated Provisions

Several provisions are designed to reduce the burden on providers. For example, they cannot be compelled to disclose records or their contents if disclosure would create an undue burden and they are immune from civil and criminal liability for complying with a court order in good faith.

6. Mandates Recommendations for Other Fiduciaries

The legislature ordered the Joint Commission on Technology and Science to develop legislative recommendations to address how other fiduciaries may access electronic communication records and digital account content.

E. Revised Uniform Fiduciary Access to Digital Assets Act

In response to the overwhelming failure of states to enact UFADAA and the growing interest in PEAC, the National Conference of Commissioners on Uniform State Laws approved the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) at its July 2015 Annual Conference. This revision is a substantial rewrite with a significant change in presumptions and procedures. Below are a few examples:

- Executors and administrators no longer have default access to the contents of e-mail. Instead, access is allowed only if the decedent consented to disclosure.
- Revised UFADAA authorizes the provider to give the user the ability to direct fiduciary access with an on-line tool such as the Facebook's Legacy

Contact and Google's Inactive Account Manager.

- No longer are terms of service prohibiting access to fiduciaries void as against public policy. Instead, the user's directions using an on-line tool have top priority followed by the decedent's directions in a will, trust, or power of attorney. If the decedent did not use an online tool or execute a document with express directions, the terms of service control.

See also Jeffrey R. Gottlieb, [*ULC Rewrites "Uniform Fiduciary Access to Digital Assets Act," Plan for the Road Ahead*](#) (July 20, 2015).

As of May 22, 2016, the RUFADAA has already been enacted in thirteen states: Arizona, Colorado, Florida, Idaho, Indiana, Maryland, Michigan, Nebraska, Oregon, Tennessee, Washington, Wisconsin, and Wyoming. In addition, it is pending in eighteen states: Alabama, Connecticut, Hawaii, Illinois, Iowa, Louisiana, Maine, Minnesota, Mississippi, New Jersey, New York, North Carolina, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Utah, and West Virginia.

F. Cases

There are few appellate court cases, although numerous media stories recount the difficulties of accessing a deceased's online accounts. In one well-publicized case, after Lance Cpl. Justin Ellsworth was killed in 2004 while serving with the United States Marine Corps in Afghanistan, his parents began a legal battle with Yahoo! to gain access to messages stored in his e-mail account. [*Yahoo Will Give Family Slain Marine's E-mail Account*](#), USA TODAY (April 21, 2005). Yahoo! initially refused the family's request, but ultimately did not fight a probate court order to hand over more than 10,000 pages of e-mails. *Id.* However, the family remained disappointed when the data CD provided by Yahoo! contained only received e-mails and none their late son had written. *Id.* A Wisconsin couple sought court orders against Google and Facebook to help them understand their 21 year-old son's suicide. Jessica Hopper, [*Digital Afterlife: What Happens to Your Online Accounts When You Die?*](#), Rock Center, June 1, 2012. Similar difficulties have

prompted state legislators to introduce legislation on the issue including the Massachusetts proposal previously discussed. *Mass. Senate Eyes Law Governing Access to the Deceased*, 90.9 WBUR (June 27, 2012).

IX. FUTURE REFORM AREAS

A. Providers Gather User's Actual Preferences

Although most Internet service providers have a policy on what happens to the accounts of deceased users, these policies are not prominently posted and many consumers may not be aware of them. If they are parts of the standard terms of service, they may not appear on the initial screens, as Internet users quickly click past them. Internet service providers should follow Google's lead and develop procedures for a person to indicate what happens upon the user's death. To ensure that more people make provisions, providers should offer an easy method at the time a person signs up for a new service so the person can designate the disposition of the account upon the owner's incapacity or death.

B. Congress Amends Federal Law

Congress should amend the Stored Communications Act and the Computer Fraud and Abuse Act to make certain that fiduciary access, even if contrary to terms of service agreements, is not potentially subject to federal criminal sanctions. Federal law could require Internet providers to respect state laws on fiduciary powers, or even to ensure that all Internet users click through an "informed consent" provision when they sign up for new services.

C. States Enact RUFADAA

State legislatures, bar committees, and other interested groups are studying RUFADAA with an eye towards enacting it "as is" or making changes from the subtle to the significant. Now that the Uniform Act has secured the approval of several major industry players such as Facebook and Google, more enactments appear very likely.

X. CONCLUSION

Complications surround planning for digital assets, but all clients need to understand the ramifications of failing to do so. Estate planning attorneys need to comprehend fully that this is not a trivial consideration and that it is a developing area of law. Cases will arise regarding terms of service agreements, rights of beneficiaries, and the ramifications of applicable state and federal laws. Until the courts and legislatures clarify the law, estate planners need to be especially mindful in planning for these frequently overlooked assets.

APPENDIX A – DIGITAL ESTATE INFORMATION SAMPLE FORM¹

DIGITAL ESTATE INFORMATION

I. LOCATIONS OF HARD COPY FILES AND MEDIA BACKUP

Personal records =

Financial =

Home/apartment records =

Media backups =

The location of traditional paper records as well as where back ups of digital information are stored is very helpful.

II. DEFAULT INFORMATION

User names =

Passwords =

Secret questions:

Mother's maiden name =

Grade school =

Street where grew up =

Many clients have default information which they use for many accounts. If no specific access information is provided, this at least provides a starting point.

Some clients may also have a method of assigning passwords. If so, the client should provide this information.

¹ For another sample form, see James D. Lamm, [*Digital Audit: Passwords & Digital Property*](#) (2012).

III. ELECTRONIC DEVICE ACCESS

<u>Device</u>	<u>Website</u>	<u>Username</u>	<u>PIN</u>	<u>Password</u>
Computer – home				
Computer – office				
Operating System				
Voice mail – home				
Voice mail – work				
Voice mail – cell phone				
Security system				
Tablet				
e-Reader				
GPS				
Router				
DVR/TiVo				
Television				

IV. E-MAIL ACCOUNTS

<u>Description</u>	<u>E-mail address</u>	<u>Username</u>	<u>PIN</u>	<u>Password</u>	<u>Disposition Desires</u>
Work					
Home					
School					

V. DOMAIN NAMES

<u>Website/Domain Name</u>	<u>Webhost</u>	<u>Username</u>	<u>PIN</u>	<u>Password</u>
Personal				
Business				

VI. ON-LINE STORAGE

<u>Name</u>	<u>Website</u>	<u>Username</u>	<u>PIN</u>	<u>Password</u>
Dropbox				
Google Drive				

VII. FINANCIAL SOFTWARE

<u>Item</u>	<u>Website</u>	<u>User Name</u>	<u>PIN</u>	<u>Password</u>
Quicken				
TurboTax				

VIII. BANKING

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>ATM PIN</u>	<u>Security Image</u>
Checking					
Savings					
PayPal					

IX. STOCKS, BONDS, SECURITIES

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>

X. INCOME TAXES

<u>Item</u>	<u>Website</u>	<u>User Name</u>	<u>PIN</u>	<u>Password</u>
Federal Income tax payment	https://www.eftps.com/eftps/			
State Income tax payment				
Prior computerized tax returns				

XI. RETIREMENT

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>

XII. INSURANCE

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>
Health				
Life				
Property				

XIII. CREDIT CARDS

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>PIN</u>
American Express				
Visa				

XIV. DEBTS

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>
Mortgage				
Cars				
Student Loan				

XV. UTILITIES

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>
Electric				
Gas				
Internet				
Phone(landline)				
Phone (cell)				
TV				
Trash				
Water				

XVI. BUSINESSES

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>
Amazon.com				
e-Bay.com				

XVII. SOCIAL NETWORKS

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Disposition Desires</u>
Facebook				
LinkedIn				
Twitter				
MySpace				

XVIII. DIGITAL MEDIA ACCOUNTS

<u>Institution</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>	<u>Other Information</u>
Netflix				
iTunes				
YouTube				
Hulu				
Nook				
Kindle				

XIX. LOYALTY PROGRAMS

<u>Name</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>
Delta			
Southwest Airlines			
Best Buy			
Office Depot			

XX. OTHER ACCOUNTS

<u>Name</u>	<u>Website</u>	<u>User Name</u>	<u>Password</u>
Skype			
LoJack			
WoW			
HalfLife			
Flickr			
Medical records			

APPENDIX B – NCCUSL’S COMPARISON OF UFADAA, PEAC, AND RUFADAA²

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


² Uniformlaws.org, [Comparison of The Uniform Fiduciary Access to Digital Assets Act \(Original UFADAA\), The Privacy Expectations Afterlife and Choices Act \(PEAC Act\), and The Revised Uniform Fiduciary Access to Digital Assets Act \(Revised UFADAA\)](#) (last visited Aug. 8, 2015).

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

Issue	Original UFADAA	PEAC Act	Revised UFADAA
Effect of boilerplate term-of-service prohibiting fiduciary access.	A blanket prohibition on fiduciary access is void as against public policy.	Not specifically addressed, but terms-of-service arguably enforceable by the reference to “other applicable law” (i.e. contract law) in Sec. 3(c).	Three tiered approach: <ol style="list-style-type: none"> 1. A user’s direction using an online tool prevails over an offline direction and over the terms-of-service <i>if</i> the direction can be modified or deleted at all times. 2. A user’s direction in a will, trust, power of attorney, or other record prevails over the boilerplate terms-of-service. 3. If a user provides no direction, the terms-of-service control, or other law controls if the terms-of-service are silent on fiduciary access.
Effect of other terms-of-service.	Not addressed.	Recipient has no greater rights than the user.	Unless they conflict with a user’s direction, terms-of-service are preserved and the fiduciary has no greater rights than the user.

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

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



Sioux Falls Estate Planning Council

**CYBER ESTATE PLANNING AND
ADMINISTRATION**

Gerry W. Beyer
Governor Preston E. Smith Regents Professor of Law
Texas Tech University School of Law

Question 1

In 2009, Colleen Burns was declared dead. Her family decided to donate her organs. As the doctors were starting to harvest her organs, she woke up and told them to stop. For how much was the hospital held liable?

- A. \$10 million.
- B. \$5 million.
- C. \$1 million.
- D. \$6,000.

2

Question 2

Scott Entsminger who died on July 4, 2013 specified that his pallbearers are to be members of a certain professional football team because he wants his team to "let him down one last time." Which team is it?

- A. Cleveland Browns
- B. Dallas Cowboys
- C. Detroit Lions
- D. New York Jets

3

Question 3

On January 20, 2013, a 101 woman woke up in her coffin right before the lid was going to be closed (she was not embalmed for religious reasons). What were her first words?

- A. WTF
- B. I'm not dead yet.
- C. Hello there.
- D. Told you zombies were real.

4

Question 4

Which of the following songs was the most popular song played at funerals in 2012?

- A. Stairway to Heaven
- B. Highway to Hell
- C. Unchained Melody
- D. Over the Rainbow
- E. My Way

5

Overview

- What are "digital assets" and "digital estates"?
- The importance of planning for these assets.
- How user policies impact the planning process.
- How Federal law impacts the planning process.
- Methods to plan for digital assets.
- Obstacles to planning for these assets.
- Fiduciary access to digital assets under current law.
- Thoughts for the future.

6

Definition of Digital Assets

"Text, images, multimedia information, or personal property stored in a digital format, whether stored on a server, computer, or other electronic device which currently exists or may exist as technology develops, and regardless of the ownership of the physical device upon which the digital asset is stored. Digital assets include, without limitation, any words, characters, codes, or contractual rights necessary to access the digital assets." [proposed Oregon statute]

7

Digital Assets -- Personal

- Types of Files:
 - Documents – word processing, pdf, etc.
 - Photos
 - Music (mp3)
 - Videos
 - Spreadsheets
 - Tax records and returns
 - PowerPoint presentations
 - e-mail and text messages
 - e-books

8

Digital Assets -- Personal

- Location of files:
 - Computer
 - Smart phone
 - Tablet
 - e-reader
 - Camera
 - Memory cards or USB flash drives
 - CDs and DVDs
 - Online in the cloud

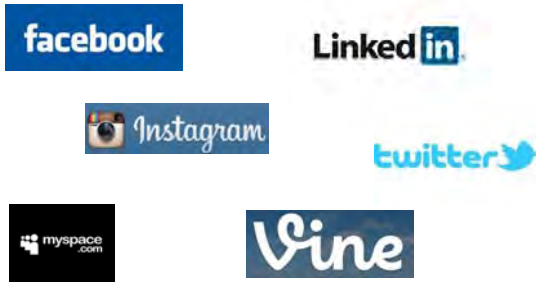
9

Digital Assets -- Personal

- Gaining access:
 - Password to start device.
 - Password to access operating system.
 - Password to open document.
 - Password to access website where material stored.

10

Digital Assets – Social Media



11

Digital Assets – Financial Accounts

- Examples:
 - Bank accounts
 - PayPal
 - Bitcoin
 - Investment and brokerage accounts
 - Utility bill payment (water, gas, telephone, cell phone, cable, and trash disposal)
 - Loan payments (mortgage, car, etc.)
 - IRS e-filing

12

Digital Assets – Business Accounts

- Examples:
 - Customer information databases (names, addresses, credit card numbers, order history, pending orders, etc.).
 - Inventory.
 - Client records (attorney, CPA, etc.).
 - Patient records (physicians, dentists, etc.).
 - eBay accounts.

13

Digital Assets – Internet Sites

- Domain Names
- Blogs

14

Digital Assets – Loyalty Program Benefits

- Examples:
 - Frequent flyer points.
 - Credit card “cash back” or “reward points”
 - Business “points,” discounts, or vouchers.

15

Digital Assets -- Others

- Gaming "money," avatars, and virtual property



16

Importance of Planning

- 1. Make things easier for your family and executor when you die or become disabled.

Life
100% fatal



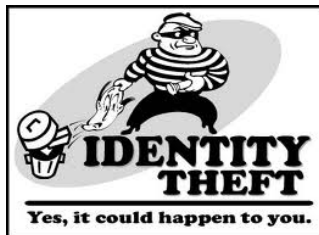
Disability > 90 days
60% chance



17

Importance of Planning

- 2. Prevent identify theft.



18

Importance of Planning

■ 3. Prevent Loss to Estate



???.com



19

Importance of Planning

■ 4. Avoid Losing the Deceased's Story



20

Importance of Planning

■ 5. Protect Secrets from Being Revealed



21

Deceased User Policies Terms of Service

- May govern what happens upon death.
- Did decedent *really* know or agree?



22

Deceased User Policies Ownership vs. License



23

Federal Law The Acts

- Stored Communications Act
- Computer Fraud and Abuse Act

24

Federal Law Interface with User Agreements

- Agreements often prohibit user from granting others access to account.
- Thus, revealing user name and password to a non-user and allowing that person to access your account may be in violation of federal statutes prohibiting access without lawful consent.

25

Federal Law Interface with User Agreements

- One enacted and some proposed statutes provide that they supersede any contrary provisions of user agreements.
- Raises issues such as:
 - Interference with contract rights.
 - Are terms of service against public policy and thus unenforceable?
 - Effect of choice of law provisions.
 - Constitutionality of such provisions.

26

Planning Suggestions

- 1. Specific Disposition According to Provider's Instructions

Google



27

Planning Suggestions

■ 2. Backup to Tangible Media



28

Planning Suggestions

■ 3. Comprehensive Inventory -- Contents

- Detailed form in the Appendix to the article

29

Planning Suggestions

■ 3. Comprehensive Inventory -- Storage

- Trusted person
- Encrypted
- Safe deposit box
- Online password storage
- **Warning:** Potential of violation of federal law:
 - Stored Communications Act
 - Computer Fraud and Abuse Act

30

Planning Suggestions

- 4. Provide Immediate Access to Portions of Digital Estate



Same warning as previous suggestion if service not designed for multiple users.

31

Planning Suggestions

- 5. Authorize Agent to Access Digital Assets



32

Planning Suggestions

- 6. Digital Asset Trust
 - Client transfers digital asset to trust
 - Digital asset must be transferable
 - Practical for valuable assets
 - Trust buys the digital assets such as license-based assets that expire upon "death"
 - Upon client's death or disability, trustee handles the asset according to the client's stated instructions (beneficiaries may use).

33

Planning Suggestions

- 7. Will
 - Do not include user names and passwords as will becomes public record.
 - Useful to transfer digital asset upon death.
 - But, asset may be governed by user policy:
 - Not transferable.
 - Ends upon death.
 - Analogous to a non-probate asset.

34

Planning Suggestions

- 8. Online Afterlife Company
 - Storage for user names and passwords.
 - Send messages upon death.
 - Send messages thereafter.
 - **Warning:** Must use due diligence to investigate. Can they do what they claim and will they be in existence when needed?

35

Obstacles to Planning

- 1. Safety
 - Computer or papers can be stolen.
 - Encryption can be broken.
 - Internet storage can be hacked.



36

Obstacles to Planning

- 2. Hassle -- Information changes rapidly:
 - Accounts opened.
 - Accounts closed.
 - Passwords change.
 - Equipment is bought and sold.



37

Obstacles to Planning

- 3. Uncertain Reliability of Afterlife Companies and Ability to do What Promised

38

Obstacles to Planning

- 4. Potential Federal Law Limitations
 - Can a fiduciary force a turnover?
 - Will provider disclose voluntarily?



Sahar Daftary

39

Fiduciary Access to Digital Assets

1. First Generation State Law

- E-mail coverage only



40

Fiduciary Access to Digital Assets

2. Second Generation State Law

- Records stored electronically



Indiana has since enacted the RUFADAA.

41

Fiduciary Access to Digital Assets

3. Third Generation State Law

- Broader coverage to include social media and microblogging



Idaho has since enacted the RUFADAA.

42

Fiduciary Access to Digital Assets

- 4. Specialized State Legislation
 - Only if deceased account holder is a minor.



43

Fiduciary Access to Digital Assets

- 5. Uniform Fiduciary Access to Digital Assets Act
 - Approved by NCCUSL on July 16, 2014
 - [Link to main UFADA website](#)



44

Fiduciary Access to Digital Assets

- 5. Uniform Fiduciary Access to Digital Assets Act
 - Applies to agents, guardians, trustees, and personal representatives.
 - Account holders have control rather than being bound by click-through terms of service.
 - Treats digital assets like all other assets.
 - Contains provisions to protect custodians of digital assets and copyright holders.

45

Fiduciary Access to Digital Assets

■ 5. Uniform Fiduciary Access to Digital Assets Act

- Enacted by Delaware effective Jan. 1, 2015.



- Introduced in 26 states and, so far, has failed in all.

46

Fiduciary Access to Digital Assets

■ 5. Uniform Fiduciary Access to Digital Assets Act

- Potential problems with UFADAA
 - Privacy concerns
 - Federal law concerns



47

Fiduciary Access to Digital Assets

■ 6. Privacy Expectation Afterlife and Choices Act

NetChoice

- Disclosure of existence of account after PR obtains a court order that records needed to resolve fiscal estate assets.
- Disclosure of contents of account after PR obtains court order that decedent's will or product settings expressly consented to after-death disclosure.

48

Fiduciary Access to Digital Assets

- 6. Privacy Expectation Afterlife and Choices Act
 - Act does not address access by other fiduciaries (e.g., agents, guardians, trustees, conservators, etc.).
 - Virginia is first (and so far only) state to enact a version of PEAC.



49

Fiduciary Access to Digital Assets

- 7. Revised Uniform Fiduciary Access to Digital Assets Act
 - In response to failure of states to enact UFADAA and industry opposition, UFADAA revised.
 - Substantial rewrite approved July 2015.

50

Fiduciary Access to Digital Assets

- 7. Revised Uniform Fiduciary Access to Digital Assets Act
 - Executors and administrators no longer have default access to e-mail contents.
 - Instead, access only if the decedent consented to disclosure.

51

Fiduciary Access to Digital Assets

- 7. Revised Uniform Fiduciary Access to Digital Assets Act
 - Encourages use of on-line tools such as Facebook's Legacy Contact and Google's Inactive Account Manager.

52

Fiduciary Access to Digital Assets

- 7. Revised Uniform Fiduciary Access to Digital Assets Act
 - Priority order for access:
 1. On-line tool directions.
 2. Directions in will, trusts, or power of attorney.
 3. Terms of service (which likely say no access).

Note: Terms of service prohibiting access to fiduciaries no longer deemed against public policy.

53

Fiduciary Access to Digital Assets

- 7. Revised Uniform Fiduciary Access to Digital Assets Act
 - Endorsements
 - Association of American Retired Persons
 - Center for Democracy and Technology
 - Facebook
 - Google
 - National Academy of Elder Law Attorneys

54

Fiduciary Access to Digital Assets

7. Revised Uniform Fiduciary Access to Digital Assets Act

2016 Introductions (enactments in green) (as of 5/22/16)

Alabama	Iowa	New York	Washington
Arizona	Louisiana	North Carolina	West Virginia
Colorado	Maine	Oklahoma	Wisconsin
Connecticut	Maryland	Oregon	Wyoming
Florida	Michigan	Pennsylvania	
Hawaii	Minnesota	Rhode Island	
Idaho	Mississippi	South Carolina	
Illinois	Nebraska	Tennessee	
Indiana	New Jersey	Utah	

55

Thoughts for the Future

- 1. Amend federal statutes
- 2. Enact comprehensive state legislation
- 3. Providers gather user's actual preferences

56

Moral

- Despite uncertainties, the prudent estate planner should plan for a client's digital assets.



57

Questions?



58
