GW Law School Public Law and Legal Theory Paper No. 2015-18

GW Legal Studies Research Paper No. 2015-18

Digital Assets and Fiduciaries

Naomi Cahn; Christina Kunz & Suzanne Brown Walsh

RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW, John A. Rothchild, ed., Edward Elger, 2016

This paper can be downloaded free of charge from the Social Science Research Network: http://ssrn.com/abstract=2603398

Electronic copy available at: http://ssrn.com/abstract=2603398

Forthcoming in John A. Rothchild (ed.), Research Handbook on Electronic Commerce Law, Edward Elgar, 2016

Digital Assets and Fiduciaries

Suzanne Brown Walsh, Christina Kunz, and Naomi Cahn[*]

Abstract:

This chapter addresses the appropriate treatment of a person's digital life when the account holder can no longer manage it. As the Internet becomes an increasingly important presence in our daily lives, the law has a significant role to play in determining the management of digital assets upon the account holder's incapacity or death. In the past, people put hard copies of photos in albums, listened to record albums, and paid bills with a stamped envelope. Today, most people use the Internet to store photos, listen to music, and pay bills. Yet few people have considered how to dispose of their digital assets.

This chapter explores the legal issues for trusts, estates, conservatorships, and powers of attorney. It addresses the importance of fiduciaries being able to manage an account holder's digital assets, and the obstacles under federal and state law to a fiduciary assuming that role. Finally, it shows how the Uniform Fiduciary Access to Digital Assets Act provides a solution to ensure effectuation of the account holder's intent.

I. Introduction: The Digital Divide

Now that we live in a digitalized world, what happens to our digital lives when we die or can no longer handle them ourselves? There are 30 million Facebook accounts that belong to dead people. The average individual has 25 passwords, and may not have ever told them to anyone else. Some service providers have explicit policies on what will happen when an individual dies, but most do not; even where these policies are included in the terms of service, most consumers click-through these agreements. Online banking and mobile banking have grown exponentially, for example. The British Bankers' Association recently released the results of a survey indicating that in the UK, bank customers make

[*]Suzanne Brown Walsh is a partner at Murtha Cullina, and she chaired the Uniform Law Commission's Drafting Committee on Uniform Fiduciary Access to Digital Assets. Christina Kunz is Emerita Professor of Law, William Mitchell College of Law, and she was an Observer to the Drafting Committee. Naomi Cahn is the Harold H. Greene Professor of Law, George Washington University Law School, and she was the Reporter for the Drafting Committee.

Electronic copy available at: http://ssrn.com/abstract=2603398

over 1 *billion* pounds of transactions electronically every day, and they have downloaded an average of 15,000 mobile banking applications each day in just the past year, alone[1]

If, instead of electronic messages or electronic records, we were dealing with physical letters or paper records, the answer would be clear. The person responsible for managing our estate, the executor or personal representative, would be in charge of rounding up our assets, destroying some, and distributing others based either on a will or the state's law of intestacy. If we were incapacitated, we could delegate authority while we were still competent to a trusted agent through a power of attorney or by establishing a trust; if we had not undertaken those actions, then a court could appoint a conservator to manage our financial matters when we became unable to do so. Each of these fiduciaries has legally enforceable responsibilities to act responsibly and loyally.

So is the situation any different when it comes to managing our digital assets? Maybe. Most states' statutes and common law governing the actions of fiduciaries fail to differentiate digital from nondigital assets, so, at first glance, digital assets appear to be treated the same as nondigital assets. However, specific state and federal laws protect privacy and criminalize unauthorized access to computers and data. Additional hurdles are generated by the terms-of-service agreements (TOSAs) and privacy policies that govern most digital accounts. A fiduciary has to surmount these obstacles in order to gain access to the digital assets of a deceased or incapacitated person.

To make sure that fiduciaries have the requisite access to digital assets, states have begun to enact legislation to address the problem, and many of the proposed state laws are modeled on the Uniform Fiduciary Access to Digital Assets Act, (UFADAA), which was approved by the Uniform Law Commission (ULC) on July 16, 2014.[2]

This chapter first explores why fiduciaries need access to digital assets when an account holder becomes incapacitated or dies. It then turns to the federal and state laws that are specific to digital assets. In the third section, it explores solutions that enable fiduciaries to manage an account holder's digital assets. Finally, it addresses common objections to fiduciary access to digital assets.

I. Why Digital Access Is Important

Consider a few cases where fiduciaries were denied information that they believed was critical. A fiduciary is often authorized to handle financial matters. Indeed, Eva Kripke was authorized to act for her husband, Sidney, under a power of attorney. He had been diagnosed with Lewy body dementia, a disease that affects cognition, movement, and emotions. For four years, she managed his online bank account—until she was informed that she had the wrong password. She tried to recover the password electronically and even provided her husband's Social Security number, but she was unsuccessful. When she

[1] Digital banking reaches £1bn a day, BBA says (2014), http://tinyurl.com/naos3zw.

[2] The act is available here: Uniform Law Commission, Fiduciary Access to Digital Assets (2015), http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets.

Electronic copy available at: http://ssrn.com/abstract=2603398

wrote to the *What's Your Problem?* column in the *Chicago Tribune*,[3] columnist Jon Yates tried to solve the problem. Ultimately, however, the bank told him that a power of attorney does not allow access to online banking and said, "You must be an account holder or user," in order to "protect the customer and mitigate risk." Ironically, perhaps, Kripke continued to be able to write checks on her husband's account and view his monthly statements even as she was denied electronic access.

A fiduciary is also responsible for winding up an estate once someone dies. Sahar Daftary's family members wanted to determine whether the model had committed suicide or had been pushed out of a window. The executor of Daftary's estate asked Facebook for access to Daftary's page so that the family could ascertain her thoughts during her final days. Facebook objected, pointing to the Electronic Communications Privacy Act, a 1986 federal law. A federal judge in California agreed that Facebook could not be required to provide access. Although Facebook wanted the court to decide whether Facebook was permitted to disclose the relevant information, the court declined to offer its opinion of federal law, instead telling Facebook to decide on its own whether release of the information would subject it to penalties.[4]

Fiduciaries need access to the digital assets of the original account holder to ensure continuity in managing the account holder's assets, to prevent identify theft, and to console family members and friends.

A. To Manage Assets

Fiduciaries are responsible for handling an individual's financial situation. This means that they may be required to (1) create an inventory of the person's assets, some of which may be digital, and many of which will be accessed through digital means; (2) operate and or wind up an individual's financial accounts, including paying the person's debts, taxes, and expenses; and (3) ensure appropriate disposition of the individual's assets, either by maintaining the status quo during any period of incapacity or by distributing the person's property to the designated beneficiaries after death.

It is now virtually impossible to collect mementos, contact friends and family, or sort through financial records without access to e-mail accounts. Most creditors and banks strongly encourage customers to "go green" and receive bills and statements electronically. Frequent flyer miles and other loyalty programs accumulate through online systems. An increasing number of people conduct all of their business and, in effect, earn their livings online, as bloggers, authors, artists, or entrepreneurs. There are now some banks and

---

[3] Jon Yates, Power of Attorney Powerless in Online Banking, Chi. Trib., May 26, 2011; http://articles.chicagotribune.com/2011-05-26/business/ct-biz-0526-problem-kripke--20110526_1_online-account-online-banking-access.

[4] Facebook Inc.'s Motion to Quash Subpoena in a Civil Case at 6-7, *In re* Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. 2012). *See also* http://www.digitalpassing.com/2012/10/11/facebook-blocks-demand-contents-deceased-users-account/ (James Lamm's blog).

financial institutions that "exist" solely online and have no brick-and-mortar branches. Both digital and nondigital accounts may be governed by TOSAs. Although the assets themselves can be available to the executor or agent, their management and transfer may require compliance with TOSAs.

Digital assets can have significant monetary value. The most obvious example is Bitcoins, a digital currency.[5] Domain names continue to garner seven- and eight-figure sales prices. In 2014, MI.com sold for $3,600,000 and whisky.com sold for $3,100,000, for example.[6] The highest price ever paid for a domain name was $35.6 million for Insurance.com in 2010, followed closely by $35 million in 2007.[7] Perhaps the most unusual, valuable digital asset sold recently was a $635,000 virtual space station in Entropia Universe, an online gaming platform.[8]

B. To Prevent Identity Theft

The Bureau of Justice Statistics, the government agency that crunches numbers for the Justice Department, recently found that 16.6 million American adults had experienced identity theft in 2012, the same year in which there were only 6.8 million nonfatal violent crimes.[9]

Fiduciaries are duly bound to preserve the assets of the estates they manage. When an individual is unable to continue to monitor his/her online accounts because of incapacity or death, it becomes easier for criminals to hack these accounts, open new credit cards, apply for jobs, and even obtain state identification cards. Thus, a fiduciary needs to monitor and protect (perhaps simply by termination) these online accounts.[10]

C. To Console Grieving Loved Ones

Many people now store their treasured photos on their computers or on dedicated websites. Geneological histories may only be available online, memoirs may be written on a computer, and recipes may be stored in online apps. Much of an individual's life story

---

[5] *See* https://bitcoin.org/en/; https://en.bitcoin.it/wiki/Introduction; Joseph Wright, *Bitcoin is Creating New Headaches for Estate Planners, Though It May Someday Cure Them*, Bloomberg BNA Electronic Commerce & Law Report (May 14, 2014); Denis T. Rice, *The Past and Future of Bitcoins in Worldwide Commerce*, Business Law Today (ABA) (Nov. 2013).

[6] *See Biggest Domain Sale in 5 Years Takes Over Top Spot on Our 2015 Year-to-Date Top Sales Chart,* http://www.dnjournal.com/ytd-sales-charts.htm (last visited Feb. 6, 2015).

[7] http://tinyurl.com/n9blpyz.

[8] *See* http://tinyurl.com/kd6pg2z.

[9] http://tinyurl.com/n72ycq3.

[10] *See* Gerry Beyer & Naomi Cahn, *When You Pass On Don't Leave the Passwords Behind,* 26 Probate & Property 40 (Jan./Feb. 2012).

may no longer be available on paper. Leonard Bernstein died in 1990, leaving the manuscript for his memoir entitled "Blue Ink" on his computer in a password-protected file. To this day, apparently no one has been able to break the password and access the document.[11]

Stories abound of grieving family members and friends searching for answers, comfort and support in the social media accounts, voicemails[12] and other digital assets of their deceased friends and relatives. For example, a teenage boy discovered the "ghost" of his deceased father in a computer game they had played together when the boy was only six years old.[13] While the monetary value of social media accounts is generally small, access to the account may be priceless to family and friends. This is what motivated teenager Eric Rash's parents, Ricky and Diane Rash, to become the driving force behind Virginia legislation that grants parents postmortem access to a minor's Facebook account content.[14]

II. Impediments to Fiduciary Access to Digital Assets

Although fiduciaries need access, digital assets present a set of distinct issues.[15] Digital assets are not the first intangible assets that estate planning attorneys have faced. Copyrights, for example, are assets regulated by federal law and capable of probate and nonprobate transfer.[16] But while copyrights clearly belong to the holder, digital assets are subject to TOSAs with another party. In addition, copyrights do not raise privacy issues, but digital communications, like traditional letters, raise privacy concerns for both sender and recipient.

A. Passwords and Encryption

[11] Helen Gunnarsson, *Plan for Administering Your Digital Estate*, 99 Ill. B.J. 71 (2011).

[12] Beth Teitell, *Preserving Voicemails Helps Modern Grieving Process*, of the Boston Globe: http://tinyurl.com/l4tvbxa.

[13] Naomi Cahn and Amy Ziettlow, *A Digital Afterlife* (Sept. 16, 2013), http://tinyurl.com/k5jxd3e;].

[14] http://tinyurl.com/pwp63mp.

[15] *See generally* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 405 (2013) (contrasting predigital searches of pockets versus smartphones).

[16] 17 U.S.C. § 201(d)(1) (2012) provides: "The ownership of a copyright . . . may be bequeathed by will or pass as personal property by the applicable laws of intestate succession"; *see* Devan R. Desai, *The Life and Death of Copyright*, 2011 WIS. L. REV. 219, 264 ("Intergenerational equity . . . may show that society's claim is greater than an author's lineal descendants."); Andrea Farkas, Comment, *I'll be Back? The Complications Heirs Face When Terminating a Deceased Author's Online Copyright Licenses*, 5 EST. PLAN. & CMTY. PROP. L.J. 411, 413 (2013) ("Many heirs are unaware that they possess such a right at all . . . .").

Most online accounts are password-protected, and the passwords can generally be reset only with access to the account holder's e-mail account (if they can be reset or recovered at all, as the Kripke story shows, above).

Moreover, access to a computer does not automatically grant the fiduciary access to the data stored on the computer's hard drive, if the passwords and the data on the computer are encrypted (as the Bernstein story shows, above).

B. Terms-of-Service Agreements (TOSAs)

Even if the fiduciary can find a password, the next hurdle is the account provider's terms-of-service agreement (TOSA), which might broadly forbid account access by anyone except the account holder[17]—implicitly barring a fiduciary from access. Online TOSAs are frequently silent as to postmortem options, or it may simply prohibit postmortem transfer. For example, Yahoo!'s terms specify:

> We know that dealing with the loss of a relative is very difficult. To protect the privacy of your loved one, it is our policy to honor the initial agreement that they made with us, even in the event of their passing.
>
> At the time of registration, all account holders agree to the Yahoo Terms (TOS). Pursuant to the TOS, neither the Yahoo account nor any of the content therein are transferable, even when the account owner is deceased. As a result, Yahoo cannot provide passwords or access to deceased users' accounts, including account content such as e-mail.
>
> Yahoo does have a process in place to request that your loved one's account be closed, billing and premium services suspended, and any contents permanently deleted for privacy.[18]

Facebook recently updated its policy on postmortem account use and access, providing for the designation of a "Legacy Contact". Facebook will still allow a personal representative or family member to obtain content with a court order via "Special Request." Once the account is "memorialized," Facebook previously would not allow anyone except the user (who presumably would then have to prove that the user has not actually died, as reported) to log into it. It did allow verified family members to request that the account be removed from Facebook. The new Legacy Contact feature provides that after the account is memorialized, a designated Legacy Contact can write a final message in a

[17] http://info.yahoo.com/legal/us/yahoo/utos/terms/ ("Yahoo grants you a personal, non-transferable and non-exclusive right and license to use the object code of its Software on a single computer . . . .").

[18] *Options available when a Yahoo Account owner passes away*, http://tinyurl.com/q76cvg8, last accessed 7/22/2014.

pinned post for your profile, respond to friend requests, and update your profile picture and cover photo. The Legacy Contact CANNOT log into the account, change past posts, photos or other things shared in a timeline, or remove any friends. [19] Google has developed its more comprehensive Inactive Account Manager[20] but most other internet service providers have been slow to develop policies relating to an account holder's incapacity.

Apple's iTunes TOSA grants the account holder a license to download and use (listen) to digital music files, but expressly prohibits their sale or transfer. This may or may not allow the user to bequeath the content or actual music files—the terms of use do not mention death.[21]

Fiduciaries are beginning to challenge TOSAs. A Massachusetts state court refused to enforce a California forum designation provision in a Yahoo! TOSA. When John Ajemian was killed in a car accident, his brother and sister, as co-executors of the estate, sought access to John's Yahoo! account in order to console grievers and then to collect estate assets.[22] Yahoo! refused to permit access to the content, even though the surviving brother had opened and originally shared access to the account; he had, however, subsequently forgotten the password.[23] Yahoo! attempted to dismiss the Massachusetts declaratory action based on the California forum designation clause; it also claimed that the e-mails weren't property of the Massachusetts estate. The appellate court held that Yahoo! was required to show that the TOSA was reasonably communicated to and then accepted by the account holder. The court's opinion discussed and differentiated between "clickwrap" agreements (requiring the user to click an "I agree" box), and "browsewrap" agreements, in which the user impliedly agrees to the posted terms by accessing the website or page or by some other conduct, but the user need not expressly agree to the terms.[24] The court concluded that without evidence that the accountholder had agreed to the TOSA, it was not enforceable. It also concluded that the estate's co-administrators were not parties to the TOSA, so they could not be bound by it. Nonetheless, the appellate court did not order Yahoo! to provide access to the content; instead, it remanded the case to the probate court to determine whether the e-mails were an asset of the estate and whether federal laws (discussed below) permitted Yahoo! to disclose them. The case indicates that restrictive TOSAs will not necessarily preclude fiduciary access, but also suggests the need to resolve other issues before fiduciary access can be presumed.

C. Privacy Policies

---

[19]. http://tinyurl.com/pmrfd2e, last accessed 3/9/2015.

[20] http://tinyurl.com/lgf25jm, last accessed 7/22/2014.

[21] *See* Apple iTunes TOSA at http://tinyurl.com/p69flak.

[22] Ajemian v. Yahoo!, Inc., 987 N.E.2d 604, 614 (Mass. App. Ct. 2013).

[23] *Id.*

[24] *See generally* Kunz, Ottaviani, Ziff, Moringiello, Porter, & Debrow, *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 Bus. Law. 279, 291 (2003).

Many online service providers and websites also post privacy policies that govern their use of the data of their customers and visitors to their websites. Privacy policies can be terms within a larger TOSA, whether set out within the TOSA, linked to the TOSA, or incorporated by reference. Alternatively, they can be free-standing agreements with the bargained-for exchange of the customer's data in return for the promised privacy protections. Lastly, they can be mere postings of policy without any force and effect as a contract. Their enforceability as contracts depends on their format and wording and, more importantly, on whether the offeree was aware of the policy (read or relied on it) and suffered provable damages from the website provider's breach of the privacy policy.[25]

U.S. law does not require companies to post privacy policies, except for financial service providers within the scope of Gramm-Leach-Bliley Act (GLBA)[26] and health care providers within the scope of the Health Insurance Portability and Accountability Act (HIPAA).[27] However, a company that posts a privacy policy and then does not follow it may be subject to an enforcement action by the Federal Trade Commission (FTC) as an unfair and deceptive trade practice.[28] The states' attorneys general have similar powers under the "little FTC Acts" in state law.[29]

D. State Trust and Estate Laws

Although statutes in every state impose legal duties on fiduciaries to act on behalf of the represented person, in administering that person's assets, only a minority of states have enacted legislation dealing with fiduciary access to digital assets. Delaware enacted a comprehensive law in 2014. Earlier state access laws, however, are limited in application, covering only personal representatives, and differing over what kinds of accounts are covered (email, social networking, blogs, etc).[30]

---

[25] Memorandum from Christina Kunz & Peter Rademacher, on Privacy Policies' Enforceability as Contracts and Their Effect on FADA (Feb. 10, 2013) (on file with Professor Kunz and with the UFADAA Drafting Committee). *See, e.g.,* Azeltine v. Bank of America (BOA), No. CV10-218-TUC-RCC(HCE), 2010 WL 6511710 (D. Ariz. Dec. 14, 2010); Smith v. Trusted Universal Standards in Electronic Transactions, Inc., No. 09-4567, 2010 WL 1799456 (D.N.J. May 4, 2010); Meyer v. Christie, No. 07-2230-JWL, 2007 WL 3120695 (D. Kan. Oct. 24, 2007); In re JetBlue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005); In re Northwest Airlines Privacy Litigation, No. Civ. 04-126 (PAM/JSM), 2004 WL 1278459 (D. Minn. June 6, 2004); Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004).

[26] 15 U.S.C. § 6803 (2012).

[27] 45 C.F.R. § 164.520 (2012) (HIPAA regulation requiring privacy policies).

[28] 15 U.S.C. § 45 (2012) (providing authority for the FTC to prevent deceptive or unfair practices); *see also* Federal Trade Commission, *Making Sure Companies Keep Their Privacy Promises to Consumers*, Fed. Trade Commission, http://www.ftc.gov/opa/reporter/privacy/privacypromises.html (last visited Feb. 2, 2013) ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises.").

[29] Jack E. Karns, *State Regulation of Deceptive Trade Practices Under "Little FTC Acts": Should Federal Standards Control?*, 94 Dick. L. Rev. 373 (1990).

[30] http://www.digitalpassing.com/2014/08/27/delaware-enacts-fiduciary-access-digital-assets-act/ (Delaware's enactment, as well as a list and descriptions of earlier state acts).

E. Federal and State Statutes Barring Unauthorized Computer Access

At the federal level, the Computer Fraud and Abuse Act (CFAA) criminalizes (or at least, creates civil liability for) the unauthorized access of computer hardware and devices, and the data stored thereon:

> (a) Whoever-- . . . (2) *intentionally accesses* a computer *without authorization* or *exceeds authorized access*, and thereby obtains-- . . . (C) information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished as provided in subsection (c) of this section.[31]

Thus, the CFAA criminalizes two kinds of computer trespass: access "without authorization" and access that that "exceeds authorized access." Although the CFAA does not define "without authorization,"[32] it defines the term "exceeds authorized access" as follows:

> to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.[33]

The unauthorized user can "obtain . . . information" by accessing emails or internet accounts from a "protected computer," which is defined as any computer connected to a government network, as well as one used in interstate or foreign commerce.[34] Since most internet servers are not located in the same state as the website's user, internet use almost always involves obtaining information from a protected computer and therefore implicates the CFAA.[35] The Seventh Circuit has clarified that "computer" includes home computers, laptops, notepads, tablets, and smartphones.[36]

Every state has an analogous statute, which varies in coverage, but typically prohibits "unauthorized access" to computers.[37]

---

[31] 18 U.S.C. § 1030(a)(2)(C) (2012).

[32] The Ninth Circuit Court of Appeals has defined "authorization" or "authorized access" to mean any permission at all. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132-33 (9th Cir. 2009).

[33] 18 U.S.C. § 1030(e)(6).

[34] *Id.* § 1030(e)(2).

[35] *See Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1127 (W.D. Wash. (2000).

[36] United States v. Mitra, 405 F.3d 492, 495-96 (7th Cir. 2005).

[37] *Computer Hacking and Unauthorized Access Laws*, Nat'l Conf. of State Legislatures, www.ncsl,org;issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (last updated June 19, 2012). For a more extensive 50-state survey of state statutes on "Unauthorized [Computer] Access/Trespass Statutes," see Memorandum

These federal and state statutes seek to deter fraudulent and criminal activity that surpasses the scope of authorization,[38] such as hacking into secured computer systems, theft of services and data, and malicious altering of computer systems and data. Even though a fiduciary is "authorized" by the account holder or state law to use a computer or to act for an account holder, the fiduciary is not necessarily exempt from CFAA prosecution.[39] Most likely, a fiduciary is "authorized" for CFAA purposes when he or she accesses the *hard drive* on an account holder's computer or system, which the fiduciary lawfully possesses, controls, or owns by virtue of the proscribed authority of a fiduciary. The analogy would be that a fiduciary using, or even hacking into, a computer is no more illegal than a fiduciary using a locksmith (or crowbar) to get into a building owned by an incapacitated person, principal or decedent. However, accessing a hard drive is vastly different than accessing the account holder's digital accounts or assets. If the fiduciary is violating the account provider's TOSA by accessing the account holder's digital accounts or assets online, the fiduciary may be violating the CFAA.

The Department of Justice (DOJ) has asserted that the CFAA gives it the right to prosecute those who violate TOSAs. Indeed, the written testimony of Richard W. Downing, Deputy Chief of the DOJ's Computer Crime and Intellectual Property Section Criminal Division, before the House Judiciary Committee Subcommittee on Crime, Terrorism, and National Security, in 2011, clearly indicated that the DOJ would like to continue to use TOSA violations to prosecute those that it unilaterally deems to be bad actors.[40]

As we know, very few people read TOSAs. Most of us open accounts and click our agreement to the TOSAs without even a cursory glance. Just to illustrate how easy it is to unintentionally violate a TOSA, an archived version of Google's TOSA (in former § 2.3) until recently prohibited minors who lacked contractual capacity from using its services.[41] The problem is that (some would say) overzealous federal prosecutors are

---

from Peter J. Rademacher & Lucie O'Neill to the Drafting Committee on Fiduciary Access to Digital Assets on Issues Pertaining to Unauthorized Access Statutes (Aug. 8, 2012) (on file with the Uniform Law Commission and with Christina L. Kunz, Professor Emerita, William Mitchell College of Law).

[38] *See generally* 18 U.S.C. §§ 2701, 1030, and the analogous state statutes. (Connecticut's computer crime law is at C.G.S. § 53a-251; it likewise criminalizes "unauthorized access.")

[39] *See* James D. Lamm, Christina L. Kunz, Damien A. Riehl, & Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. MIAMI L. REV. 385 (2014).

[40] *See Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 5, 14 (2011) (statement of Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Dept. of Justice). Cached copy of testimony available at: http://tinyurl.com/k2nv3o3 (emphasis added). *See also* Jim Lamm, *Planning Ahead for Access to Contents of a Decedent's Online Accounts*, DIGITAL PASSING (Feb. 9, 2012), http://www.digitalpassing.com/2012/02/09/planning-ahead-access-contents-decedent-online-accounts/ (referencing state felony charges against defendant for accessing his wife's gmail account). *Cf.* United States v. Nosal, 676 F.3d 854, 860, 862 (9th Cir. 2012) ("The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor.").

[41] http://tinyurl.com/mextubw.

using the CFAA to prosecute defendants based solely on violations of a website's TOSA.[42] Until Congress amends and clarifies the CFAA, the scope and breadth of the CFAA's reach will remain unclear, including its impact on fiduciaries just trying to perform their statutory duties. And that lack of clarity will continue to have a chilling effect on fiduciaries, as they attempt to deal with the digital assets of account holders.

F. The Stored Communications Act

The Fourth Amendment of the United States Constitution provides citizens with a strong expectation of privacy in their homes. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . .") As a result, the government cannot normally search our homes without first showing probable cause and obtaining a search warrant authorizing a search.

When we use a computer network, we may have the same personal expectation of privacy, but the network is not physically located or even being accessed within our computers or in our homes, so it is outside the coverage of the Fourth Amendment. To fill that gap, Congress enacted the Stored Communications Act (SCA) in 1986, as a part of the Electronic Communications Privacy Act (ECPA),[43] to respond to concerns that internet privacy posed new dilemmas with respect to application of the Fourth Amendment's privacy protections. The privacy protections of the SCA prohibit certain providers of *public* communications services from disclosing the *contents* of its user's communications to a government or nongovernment entity (different rules apply to each), except under limited circumstances which are akin to the "warrant" required under the Fourth Amendment. It regulates the relationship between the government, internet service providers (ISPs), and users in two distinct ways.

First, the SCA establishes limits on the government's ability to require ISPs to disclose information concerning their subscribers. An ISP may not disclose to the government any records concerning an account holder or the contents of any electronic communications, in the absence of an applicable exception, such as consent by the account holder.[44]

---

[42] *See* Washington Post article entitled, "The Law Used to Prosecute Aaron Swartz Remains Unchanged a Year After his Death" found online at http://tinyurl.com/otpk3d2.

[43] The SCA is codified at 18 U.S.C. §§ 2701-2711. *See generally* Orin Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. 1208 (2004).

[44] 18 U.S.C. § 2702(a)(1) prohibits voluntary disclosure to anyone of the contents of an electronic communication, while 18 U.S.C. § 2702(a)(3) prevents the voluntary disclosure of records to the government (although not to others). Depending on the nature of the data, the government must obtain either a subpoena or a warrant, although there are some exceptions in the case of an emergency. 18 U.S.C. § 2702(b).

Providers are permitted, but not required, to divulge non-content information, such as the user's name, address, connection records, IP address, and account information to a non-governmental entity.[45]

Second, the SCA establishes limits on the providers' ability to voluntarily disclose the contents of communications to the government or any other person or entity.[46] Although the drafters tried to cover future developments, at the time of the SCA's enactment, the internet did not yet exist, the development of Facebook was still almost two decades away, the founding of Google was more than a decade in the future, and even the large-scale use of email was still a few years distant.[47] The drafters were focused on privacy, not on how the SCA might affect fiduciary property management and distribution,[48] and the SCA has not been amended since its original enactment. (Of course, few people recognized the potentially transformative potential of the internet on trusts and estates practice at that point.) The resulting uncertainty affects anyone with an email account. It hampers fiduciaries, including personal representatives, conservators, agents acting pursuant to a power of attorney, and trustees who want to obtain access to any type of electronic communication, although it does not affect the ability of a fiduciary to distribute the assets held in the underlying account—once the fiduciary has been able to identify and access it. Private social media account contents (photos, videos, posts) are probably all "communications" protected by the SCA.[49]

If the provider of the electronic communications service provides the service only to employees or students, but not to the general public, that provider is not subject to the

---

[45] *Id.* § 2702(c)(6).

[46] *See* Kerr, *User's Guide*, *upra* note 44, at 1212-13 ("The statute creates a set of Fourth Amendment-like privacy protections"). The 2013 revelations of Edward Snowden provide another angle on the SCA and providers' willingness to disclose. The ISPs did not want to disclose some information, and the NSA either coerced them or simply took it without their knowledge. *See, e.g.*, Ryan Lizza, *The Metadata Program in Eleven Documents*, THE NEW YORKER (Dec. 31, 2013), http://www.newyorker.com/online/blogs/comment/ 2013/12/a-history-of-the-metadata-program-in-eleven-documents.html#slide_ss_0=1, *archived at* http://perma.cc/ 8R7Y-GBAE; Ryan Lizza, *State of Deception*, THE NEW YORKER (Dec. 16, 2013), http://www.newyorker.com/reporting/2013/12/16/131216fa_fact_lizza, *archived at* http://perma.cc/ F4KK-FVXG; Laura W. Murphy, *The NSA's Winter of Discontent*, HUFFINGTON POST (Dec. 12, 2013, 5:59 AM), http://www.huffingtonpost.com/laura-w-murphy/the-nsas-winter-of-discon_b_4434455.html, *archived at* http://perma.cc/3V8U-6X6W.

[47] Ian Peter, *The History of Email*, NETHISTORY, http://www.nethistory.info/ History%20of%20the%20Internet/email.html, *archived at* http://perma.cc/ EP9X-9JQA (last visited Sept. 8, 2014); *see* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1198 (2010) ("It was on the cusp of this phase, with computer networking in its infancy, that Congress adopted the Stored Communications Act in 1986."); Michael Helft & Claire Cain Miller, *1986 Privacy Law is Outrun by the Web*, N.Y. TIMES, Jan. 9, 2011, http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=all&_r=0, archived at http://perma.cc/4-2HL4.

[48] At the time of promulgation of the Uniform Fiduciary Access to Digital Assets Act in July 2014, only one reported federal case dealt with the relationship between the SCA and probate. *In re* Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. 2012).

[49] *See* Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259 (2012).

SCA and cannot use its provisions to justify refusing to honor a request by a fiduciary (or by a government entity) for copies of communications or access to an account. (An employer might have other obvious reasons to want to or need to prohibit access to employer-provided accounts by a fiduciary or law enforcement without a warrant or a court order, but the SCA's prohibitions against what is the equivalent of a warrantless search do not apply.)

Note that the SCA applies different rules to government entities (mainly law enforcement) requesting information, versus all others (such as fiduciaries). Under the SCA, law enforcement officials can force or compel a provider who is otherwise covered by the SCA to divulge account contents.[50] A fiduciary, however, can never compel the provider to divulge the same information.

A provider of electronic communications services to the public can *voluntarily* disclose the contents of communications, but only if an *exception* to the SCA's blanket prohibition against disclosure applies.[51] The relevant exception for fiduciaries permits a provider to disclose communication contents if it has the "lawful consent" of "the originator" or an addressee or intended recipient of such communication[s], or the subscriber.[52] However, some providers are still balking at granting executors access to the content of decedents' e-mail accounts, without the added assurance of a court order stating that the executor has the user's lawful consent.

That is why Facebook, in its memo supporting Facebook's motion to quash a civil subpoena for information contained in a deceased user's profile and account, essentially asked one court to alternatively hold that the fiduciary had lawful consent and to order Facebook to disclose the requested content.[53] The court granted Facebook's motion to quash the subpoena, but refused to address whether Facebook could voluntarily disclose the content.[54]

A federal jury in Massachusetts awarded a plaintiff significant monetary damages in a civil action brought under the SCA. The defendant had been given the plaintiff's e-mail account password, so she could access it to read consultation reports when the two parties practiced medicine together. When the defendant left the practice and a business dispute arose, she used the plaintiff's unchanged password to access the account for reasons connected to the business dispute. The plaintiff sued, alleging that the defendant's later access was unauthorized under the SCA. Despite very thin (or nonexistent) testimony

[50] 18 U.S.C. § 2703.

[51] *Id.* § 2702(b).

[52] *Id.* § 2702(b)(3).

[53] *Facebook, Inc.'s Motion to Quash Subpoena in Civil Case*, No. C 12-80171 LHK (N.D. Cal. Aug. 6, 2012).

[54] *In Re Request for Order Requiring Facebook, Inc., to Produce Documents and Things*, No. C 12-80171 LHK (N.D. Cal. Sept. 20, 2012).

to support the damage claim, the jury awarded the plaintiff $450,000 for the unauthorized intrusion.[55]

G. Intellectual Property and Data Protection Statutes

Other bodies of law might impede a fiduciary from downloading or distributing another person's digital files. For instance, such an action may violate copyright law or trade secret law.

Another set of impediments can arise from the limited common law of privacy, and federal and any state personal data protection statutes. For example, Massachusetts has a data security statute which requires encryption of personal information "owned or licensed [held by permission]" by any person.[56] According to the National Conference of State Legislatures, 47 states have enacted laws on data security breach notifications.[57]

III. Planning for Fiduciary Access to Digital Assets

A. Digital Asset Awareness

At a minimum, clients need to be advised to develop an inventory of digital assets, including a list of how and where they are held, along with usernames, passwords, and password "prompts." Lawyers can provide advice on the what happens without planning as well as on the choices for opting out of the default systems.[58]

Needless to say, a will should not contain passwords or other critical information about digital assets, because wills are not generally immediately available, and they must be publicly filed in a court or with a registrar. In any event, any password information in a will likely be obsolete by the time it is probated.

To prevent identity theft, security experts advise us to use a different password for each website, change passwords frequently, and use random combinations of numbers and letters. Since that is impossible for mortals, most people use the same few passwords over and over. Alternatively, there are dedicated password memorization programs that you install on your computer which can memorize all of your passwords for you, requiring you to learn only one master password for the master program.

---

[55] Jury Verdict Form at 1-3, *Cheng v. Romo*, No. 11-cv-10007-DJC, 2013 WL 2245312 (D. Mass.); *Cheng v. Romo*, No. 11-1007-DJC, 2012 WL 6021369, at *1-3 (D. Mass. Nov. 28, 2012).

[56] *See* 201 CMR 17.00 (requires businesses to encrypt sensitive personal information about Massachusetts residents that is stored on portable devices such as PDAs and laptops or on storage media such as memory sticks and DVDs).

[57] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[58] *See* the "Virtual Asset Instruction Letter" or "VAIL" at http://tinyurl.com/mwbfanp, developed by Victoria Blachly of Samuels Yoelin Cantor in Oregon, for a good example of a client checklist. Jim Lamm also has made his "Digital Audit" template available on http://tinyurl.com/pez63dr.

B. E-Mail is Fundamentally Different than Paper Correspondence.

E-mail messages enjoy the same property and copyrights as pen and ink letters.[59] "If a deceased leaves behind a computer hard drive containing copies of e-mail messages, these messages would pass to the next of kin just as would a shoebox full of old letters. Heirs might similarly inherit previously printed copies of e-mail messages. However, the copyright in these messages would pass separately and independently to the heirs either [by will or intestacy]."[60] Just like a paper letter, the author who owns the copyright in a sent message cannot compel the recipient to return it, but can prevent the recipient from reproducing, distributing or displaying it.[61]

However, e-mails are unlike traditional letters in several ways. As compared to paper letters, lost e-mails might be more easily located and retrieved from an e-mail service provider. Access to e-mails might be important, perhaps for literary value, but more likely because a decedent's e-mail account contains the information necessary to continue a business or collect other assets. E-mails concerning financial and business accounts can be quite time-sensitive.

An employer might deny a fiduciary access to an employer-provided e-mail account for a number of reasons, especially business secrets and confidentiality of one sort or another. With luck, the employer will be willing to search an employee's account at the family or fiduciary's request, to ensure that the e-mails do not contain "protected" information before turning it over.

C. Estate Planning Documents Should Properly Address Digital Assets.

Some digital assets have value, at least while the owner is alive and can access them. So, the estate and trust lawyer's natural reaction is to assume that all digital assets behave and are legally treated just like their brick-and-mortar counterparts. However, not all digital assets are transferable on death. Depending on the nature of the digital asset and the TOSA, the ISP may or may not recognize a traditional will or trust as validly transferring either access to, or ownership of, the account.

Not so long ago it was much more difficult for one person to give another access to bank and financial accounts during incapacity. At a minimum, a written, notarized durable power of attorney or joint/agency bank or trust account was required, and often a company-specific certification was required. Today, the unofficial solution is to transfer the online password, even though it does not satisfy the official requirements of the financial or online institution and might violate the TOSA and the CFAA.

---

[59] Darrow & Ferrera, *Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?* 10 N.Y.U. J. Legis.& Public Policy 281, 289 (2007).

[60] *Id.* at 299.

[61] *Id.*

It is important to expressly grant the fiduciary power over digital assets and to include provisions for the disposition of digital assets with monetary or sentimental value. If the client wants particular digital assets to be destroyed, encrypted, or otherwise protected from disclosure, that direction should be accompanied by a corresponding exculpation provision. Until the federal privacy and fraud and abuse laws expressly recognize fiduciary authority, there may be civil or criminal liability associated with any third-party access to digital accounts, as discussed above. In addition, while well beyond the scope of this outline, fiduciary destruction of an otherwise valuable asset, even at the decedent's direction, may be unwise, as the fiduciary's duties to the beneficiary may be paramount.[62]

In April 2013, Google introduced an option called "Inactive Account Manager" to allow users to determine (within preset options) what will happen to their Google accounts after a predetermined period of inactivity. Users can set the time period of inactivity that triggers a Google response, and Google will also alert the user by text and e-mail one month before deleting the account. Users may have Google notify up to ten "beneficiaries" that the account will be closed, before Google deletes it. After the recipients receive that notice, those designated "beneficiaries" can download the user's Google content (such as gmail, photos or YouTube videos and blogs). Or, the user can simply instruct Google to delete all account content.[63] This feature is a step forward, even though it will not assist with postmortem access if it is not used by the account holder before death, or if the designated "beneficiary" is unavailable, incapable or dead.

IV. Estate Administration of Digital Assets

A. Checklist of Basic Steps

Victoria Blachly, an observer on the ULC's UFADAA Drafting Committee, suggests that personal representatives take the following eight steps to address a decedent's digital assets:

1. Get technical help if necessary.
2. Consolidate virtual assets to as few "platforms" as possible (e.g., have multiple e-mail accounts set to forward to a single e-mail account.)
3. Obtain statements (or data) of the prior 12 months of the decedent's important financial accounts.
4. Consider notifying the individuals in the decedent's e-mail contact list and other social media contacts.
5. Change passwords to those that the fiduciary can control (and remember).
6. Keep all accounts open for some period of time to make sure all relevant or valuable information has been saved and all vendors or other business

[62] *See* Strahilevitz, *The Right to Destroy*, 114 Yale L.J. 781 (2005), available for download at http://tinyurl.com/mucjola.

[63] http://tinyurl.com/l6mqpkz.

contacts have been appropriately notified, and so all payables can be paid and accounts receivable have been collected.
7. Remove all private and/or personal data from online shopping accounts (or close them as soon as reasonably possible).
8. Plan on archiving important electronic data for the full duration of the relevant statutes of limitations.[64]

Of course, much of this assumes that the fiduciary is granted full access, control and authority over the decedent's accounts, and is thereby deemed an "authorized user" with "lawful consent," who steps into the decedent's shoes for all purposes. Ultimately, fiduciaries need to be aware of digital assets and who is controlling them in order to determine whether their disposition comports with the decedent's estate plan.

B. Effectuating a Decedent's Intent

Some decedents may have wanted to prevent postmortem access to, or publication of, the content of their digital accounts. Some will, no doubt, figure out how to block family or fiduciary access by using an account manager feature such as Google's, or a digital estate planning service. Or, they may entrust their password and deletion instructions to a friend or advisor. (A superb password or encryption might work to protect data on a hard drive, but it would not provide foolproof protection for data stored on a service's server.) What about the decedent who leaves evidence that his/her intent was to prevent access or mandate the destruction of all content in an account, but fails to leave the login or password information? Some experts suggest that a client who wishes to maintain their privacy after death should use a secret account, because heirs who are unaware of it cannot request access to its contents.[65]

The situation becomes more complicated when the content the decedent directs to be destroyed has monetary value. It would seem that situation should be treated no differently than that of a celebrity or famous author who mandates the destruction of printed files.

C. Protecting the Decedent's Identity

A fiduciary must take basic precautions against identity theft, including cancelling credit and charge accounts as soon as possible; sending copies of death certificate to the three credit-reporting bureaus (Equifax, Experian and TransUnion); obtaining free credit reports from each credit bureau to ensure no post-death activity; and cancelling the decedent's driver's license at the motor vehicle department and asking the department to refuse any requests for duplicates.

---

[64] Michael Walker & Victoria D. Blachly, *Virtual Assets*, ST003 A.L.I.-A.B.A. 175, 177 (2011).

[65] Darrow and 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, 315 (2007).

V. Ensuring Access

While estate planning documents can set out an account holder's preferences, the absence of state or federal law allowing fiduciary access means that no one can guarantee that the account holder's intent will ultimately control (think back to Eve Kripke's experience).

UFADAA seeks to place the fiduciary into the shoes of the account holder through a variety of provisions, resolving as many of the impediments to fiduciary access to digital assets as possible.: it defines digital assets, provides default rules, defers to account holder intent and privacy desires, and encourages custodian compliance. It (1) specifies that the fiduciary is deemed to have the account holder's lawful consent, so as to ensure SCA compliance in the release of the contents of electronic communications ; (2) clarifies that if any digital material was illegally obtained by the decedent, then the fiduciary's attempt to take control of it will not "launder" it to pass clean title to the heirs; and (3) sidesteps contentious issues about whether a fiduciary can challenge restrictive terms of service precluding transfer or specifying choice of law.[66] The Act includes one right for the fiduciary that goes beyond the rights of the account holder: if the SCA permits the ISP to disclose, then the UFADAA requires the ISP to do so in order to ensure fiduciary access and ease of administration, so that the fiduciary has the same knowledge base as the account holder.[67]

UFADAA was drafted with the assistance of participating observers from several state bar committees drafting legislation, and from NAELA, ACTEC, Facebook, Google, Yahoo, NetChoice, Microsoft, The Verge, Northern Trust, the American Bankers' Association, and representatives from the gaming industry. While some industry observers objected to some UFADAA provisions, the approved act differentiates between electronic mail content that is protected by the SCA and other content, as they had requested.

A. Key Concepts and Definitions

UFADAA covers personal representatives, conservators, agents acting under powers of attorney, and trustees. It defines the fiduciary as an authorized user and thereby gives the fiduciary the authorization to access digital files under (the first section, 18 U.S.C. § 2701) of the SCA, as well as under the CFAA. It gives the fiduciary "the lawful consent" of the originator/subscriber so that the provider can voluntarily disclose the files pursuant to the

[74] In general, a fiduciary can assert whatever rights could be asserted by the account holder, subject to recognition of the indescendibility of certain types of claims. *See, e.g.*, *Ajemian*, 987 N.E.2d at 614 (allowing co-administrators of the decedent's estate to challenge a forum selection clause in a TOS agreement); Horton, *supra* note 28, at 570 ("[UFADAA] would give personal representatives nearly the same dominion over virtual assets that they enjoy over chattels and real estate."). One concern at drafting committee meetings was fiduciaries' efforts to access and then possibly transfer, illegally obtained property, such as pirated material. There are potentially interesting analogies to digital property in the gun area. *See also* Lee-Ford Tritt, *Dispatches from the Trenches of America's Great Gun Trust Wars*, 108 NW. U. L. REV. 154, 175 (2013) (discussing the utility of gun trusts in the federal law context of firearm regulation); Nathan G. Rawling, Note, *A Testamentary Gift of Felony: Avoiding Criminal Penalties from Estate Firearms*, 23 QUINNIPIAC PROB. L.J. 286, 287-90 (2010) (noting the interplay of federal and state law in firearm ownership).

[75] UNIFORM LAW COMM'N, FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 9 (2014). This has been a particularly contentious provision.

second relevant provision of the SCA (18 U.S.C. § 2702). Moreover, this language should be adequate to avoid liability under the state unauthorized access laws.

UFADAA grants fiduciaries access to digital assets that is limited to that necessary to carry out their duties; clearly, it is not personal access and does not allow a fiduciary to maintain or continue social media accounts by "impersonating" the account holder for whom the fiduciary is acting.

The Act's definitions provide the tools for understanding its scope. Section 2(1) defines an "account holder" as a person who has entered into a TOSA with a custodian, or a fiduciary for such a person. Section 2(8) defines a custodian as "a person that carries, maintains, processes, receives or stores a digital asset of an account holder." Under Section 2(9), a "digital asset" is a record that is electronic, not including an underlying asset or liability unless the asset or liability is itself a record that is electronic. This includes both the catalogue, or log, of electronic communications and the content of electronic communications, but it would exclude securities or currency. For example, consider an online commodities account for purchasing gold bullion. The digital assets covered by UFADAA are the records concerning the account, not the gold bullion itself. Ownership of the bullion is not affected by the fiduciary's access to records about the account, even though a transfer of title might occur electronically under other law. Securities held in street name or money in a bank are not digital assets; UFADAA reinforces the fiduciary's right to access all relevant electronic communications and the online account that provides evidence of ownership.

The term, "*content* of an electronic communication," merits its own definition, in Section 2(6): it is information concerning the *substance or meaning* of the communication, which has been sent or received by an account holder, is not readily accessible to the public, and is in electronic storage by a custodian providing an electronic-communication service to the public (and is therefore "covered" and "protected" by the SCA). Other electronic-communication (EC) content (not protected by the SCA) is instead included in the broader definition of a "digital asset," in Section 2(9), described above.

B. Fiduciaries' access

Each fiduciary is addressed separately.

1. Personal representatives: UFADAA Section 4 gives the personal representative access to digital assets, unless the decedent prevented access in a TOSA election that complies with Section 8(b) or in a will, or a court otherwise prohibits access. In deference to custodians' unease as to the availability of fiduciary authority under SCA, personal representatives have access to EC content only if disclosure is permitted under federal law.

2. Conservators (including Guardians): Section 5 permits a court to authorize conservator access to digital assets after the opportunity for a hearing. Disclosure of EC content may only be ordered if permitted under federal law. State law will most likely require the court to consider the protected person's intent, best interest and

personal values. Social media companies object to ongoing use of account, as opposed to limited access, which is why the Act speaks of "access" and not management.

3. Access by Agents Acting under Powers of Attorney: Section 6 provides that, unless prohibited by the principal, an agent has access to the most of the principal's digital assets and the catalogue of the principal's electronic communications. *However, the Act does NOT give an agent default authority over electronic communications content*, so this authority is akin to gifting, in that the principal must expressly include the authority in order to grant access. Although there was lengthy debate about this policy on the floor of the annual meeting, ultimately the Commission voted to track the SCA, which requires the account holder's lawful consent. For that reason, UFADAA makes access to EC content by an agent a "hot" power (meaning that it has to be specifically granted by the principal).

4. Access by Trustees: Section 7 provides that trustees who are original account holders can access all digital assets held in the trust. There should be no question that a trustee who is the original account holder will have full access to all digital assets. For assets that are transferred by the settlor or otherwise, a trustee is not the original account holder of the digital assets, and the trustee's authority is qualified and is governed by Section 7(b). Although that act of designation or transfer of the legal title should supply the necessary "lawful consent" under federal law, Section 7(b) distinguishes between access to EC content and the EC catalogue when the trustee is not the original account holder, just to be safe.

In all cases, the settlor is free to prevent trustee access to his or her digital assets in the trust instrument or by a TOSA election that complies with Section 8(b), or a court can prohibit access, based on privacy concerns.

UFADAA does not contain provisions facilitating the transfer of digital assets into a trust. That access and transfer would be accomplished by the settlor (while alive and capable), the settlor's agent, or a personal representative.

Underlying trust documents or default trust law generally supplies the allocation of responsibilities among trustees. Therefore, drafters should consider access to digital assets, as well, when drafting trustee powers provisions.

C. Fiduciary Authority

UFADAA Section 8 specifies the nature, extent and limitation of the fiduciary's authority over digital assets. Subsection (a)(1) establishes that the fiduciary is authorized to exercise control over the account holder's digital assets, but only to the extent of the account holder's authority and the fiduciary's powers, and subject to the TOSA, other applicable laws, such as copyright. Subsection (a)(2) says that the fiduciary has the account holder's lawful consent under applicable electronic privacy laws. Subsection (a)(3) further specifies that the fiduciary is an authorized user under any applicable law on unauthorized computer access.

The fiduciary has the same authority as the account holder except where, under subsection (b), the account holder has affirmatively and separately agreed to a TOSA provision denying fiduciary access. Otherwise, a TOSA provision that limits fiduciary access is declared to be void as against public policy. The drafting committee felt this was absolutely necessary, given the reality of widespread user ignorance of TOSA provisions.[68]

Subsection (b)(2) reinforces the "stepping into the shoes" nature of fiduciary authority by indicating that the fiduciary's access, by itself, will not violate a TOSA provision prohibiting third-party access or deem fiduciary access to be a transfer. This will prevent prosecutions based solely on the fiduciary's access, which would otherwise be authorized but would technically violate the TOSA and thus, the CFAA.

Subsection (c) further secures the results under subsections (a) and (b) by rendering unenforceable any TOSA choice-of-law clause that prevents fiduciary access.

Subsection (d) clarifies that the fiduciary is authorized to access digital assets stored on devices, such as computers or smartphones, without violating state or federal laws on unauthorized computer access.

If a fiduciary has access under UFADAA and substantiates his or her authority as specified, a custodian must comply with the fiduciary's request for access, control, or a copy of the digital asset. Consequently, if federal law permits the custodian to disclose, UFADAA requires disclosure. In exchange, Section 10 immunizes a custodian who complies with the request.

Section 3(b) provides that the Act does not apply to digital assets of an employer used by an employee in the ordinary course of the employer's business. This language is intended to preclude fiduciary access to employer-provided e-mail systems and employer data. By implication, it allows fiduciaries to access employees' personal accounts that are not used for business. So, for example, a Yahoo! employee's fiduciary would not have access to the employee's business e-mail or other accounts, but potentially could access the employee's personal Yahoo! account.

D. Objections

[68] For a recent example, see http://tinyurl.com/ng8379o: "Londoners give up eldest children in public Wi-Fi security horror show," reporting about Londoners connecting to free public Wi-Fi who were asked to approve terms and conditions which included a "Herod clause" promising the free Wi-Fi, but only if "the recipient agreed to assign their first born child to us for the duration of eternity". Six people signed up.

The primary objections to fiduciary access focus on preserving the privacy of the account holder.[69] For example, Yahoo! has raised the following arguments against the proposed uniform legislation:

> First, it does not ensure the privacy of sensitive or confidential information shared by the decedent or third parties. Second, [it] is based on the faulty presumption that the decedent would have wanted the trustee to have access to his or her communications.[70]

Preserving an account holder's privacy is just as important in the digital world as it is in the non-digital world. Allowing fiduciary access ultimately preserves the account holder's privacy and treats digital assets like other assets, because fiduciaries have legally enforceable responsibilities and because the account holder can establish the level of privacy she prefers.

First, in all states, existing law specifies that the fiduciary is subject to the duties and obligations established pursuant to state fiduciary law and is liable for breach of those duties. Accordingly, these laws prohibit any fiduciary from violating fiduciary responsibilities by divulging or publicizing any information the fiduciary obtains while carrying out his or her fiduciary duties**.** Fiduciaries who discover private or sensitive information about either the account holder or a third party must protect that information, or they may be subject to a claim for breach of their fiduciary duty or even a breach of privacy claim by the third party.

In exercising its responsibilities, the fiduciary is subject to the same limitations as the account holder. For example, a fiduciary cannot delete an account if this would be fraudulent. So, even if the digital asset were illegally obtained by the account holder, the fiduciary would still need access in order to handle that asset appropriately. There may, for example, be tax consequences that the fiduciary would be obligated to report. The fiduciary also gains the rights of the account holder. Similarly, if the account holder could challenge provisions in a TOSA, then the fiduciary is also able to do so.

Moreover, every fiduciary has obligations of good faith and loyalty, including protecting the account holder's privacy. Each of the fiduciaries is subject to different opt-in and default rules based on the presumed intent of the account holder and the applicability of other state and federal laws. A personal representative is presumed to have access to all of the decedent's digital assets unless that is contrary to the decedent's expressed intent or to other applicable law. A conservator may access digital assets pursuant to a court order. An agent acting pursuant to a power of attorney is presumed to have access to all of a principal's digital assets not subject to the protections of other applicable law; if another law protects the asset, then the power of attorney must explicitly grant access. And a

---

[69] Letter, http://netchoice.org/wp-content/uploads/Industry-Veto-Request-of-DE-HB-345-Signed.pdf.

[70] Bill Ashworth, Your Digital Will: Your Choice, http://yahoopolicy.tumblr.com/post/97570901633/your-digital-will-your-choice.

trustee may access any digital asset held by the trust unless that is contrary to the terms of the trust or to other applicable law.

Second, under UFADAA, default rules of access may be altered by the account holder through a will or other document or by an affirmative online act. Some ISPs already allow the account holder to direct the custodian on how to dispose of the account holder's digital assets, specifying to whom they may (or may not be) released. Accordingly, the account holder can determine the level of appropriate protection for herself, rather than relying on standard-form TOSAs.

VIII. Conclusion

As we live more of our lives online, important parts of our lives continue to live online, when we die. Legally appointed fiduciaries need to access our online lives in order to delete, preserve, and pass along digital assets as appropriate. Estate planning attorneys are increasingly advising their clients of the importance of planning for their digital assets just as they plan for their non-digital assets. And the laws on trusts and estates (and other fiduciaries) are moving slowly towards ensuring appropriate fiduciary access.