NAELA JOURNAL

National Academy of Elder Law Attorneys • Volume 12 • Number 2 • Fall 2016

The Revised Uniform Fiduciary Access to Digital Assets Act: Striking a Balance Between Privacy Expectations and the Need for Fiduciary Access to Digital Assets

By Suzanne Brown Walsh, JD, and Catherine Anne Seal CELA, CAP

NAELA™
National Academy of Elder Law Attorneys, Inc.

NAELA Journal (ISSN 1553-1686) is published twice a year by the National Academy of Elder Law Attorneys, Inc., 1577 Spring Hill Road, Suite 310, Vienna, VA 22182, and distributed to members of the Academy and to law libraries throughout the country.

Elder and Special Needs Law topics range over many areas and include: Preservation of assets, Medicaid, Medicare, Social Security, disability, health insurance, tax planning, conservatorships, guardianships, living trusts and wills, estate planning, probate and administration of estates, trusts, long-term care placement, housing and nursing home issues, elder abuse, fraud recovery, age discrimination, retirement, health law, and mental health law.

Articles appearing in *NAELA Journal* may not be regarded as legal advice. The nature of Elder and Special Needs Law practice makes it imperative that local law and practice be consulted before advising clients. Statements of fact and opinion are the responsibility of the author and do not imply an opinion or endorsement on the part of the officers or directors of NAELA unless otherwise specifically stated as such.

A subscription to *NAELA Journal* is available to law libraries for $70 per year. A combined subscription to *NAELA News*, distributed four times a year, and *NAELA Journal* is available to law libraries for $135 per year. Back issues of *NAELA Journal* and *NAELA News* are available to NAELA members and subscribing law libraries in electronic format on www.NAELA.org. Address changes or other requests regarding subscription information should be directed to Nancy Sween, Sr. Director of Communications and Publications, nsween@naela.org.

The Revised Uniform Fiduciary Access to Digital Assets Act: Striking a Balance Between Privacy Expectations and the Need for Fiduciary Access to Digital Assets

By Suzanne Brown Walsh, JD, and Catherine Anne Seal CELA, CAP

I. Introduction[1]

In the past, fiduciaries responsible for managing people's assets could easily marshal, collect, and manage these assets. Often, the biggest nuisance was convincing a recalcitrant financial institution to honor a power of attorney, and personal representatives and conservators, armed with court decrees, encountered few problems. That landscape has changed with the advent and popularity of digital assets and accounts.

According to a 2010 Pew Research Center survey, 81 percent of nondisabled adults and 54 percent of adults living with a disability use the internet.[2] According to a 2013 Pew survey, 59 percent of Americans age 65 and older use the internet, almost half have a high-speed broadband connection at home, and more than three-quarters have a cell phone.[3] Despite this, few online account custodians offer customers online tools that allow them to provide for access to, or disposition of, any property held in such accounts or even access to the records associated with the accounts. In addition, only a few state probate codes provide rules that apply in the absence of any planning. Delaware enacted a comprehensive access law in 2014.[4] Ear-

1 This article is based on an article co-authored by Suzanne Brown Walsh — *Digital Assets and Fiduciaries*, by Naomi Cahn, Christina L. Kunz, and Suzanne Brown Walsh (Research Handbook on Electronic Commerce Law (John A. Rothchild ed., Edward Elger 2016), http://ssrn.com/author=2394675. We are also deeply indebted to attorney James Lamm of Minneapolis and to Benjamin Orzeske of the Uniform Law Commission for their continuing work on the Uniform Fiduciary Access to Digital Assets Act (UFADAA), the Revised UFADAA, and the issues discussed in this article.

2 Susannah Fox, Americans Living With Disability and Their Technology Profile, PewResearchCenter, http://www.pewinternet.org/2011/01/21/americans-living-with-disability-and-their-technology-profile (Jan. 21, 2011).

3 Aaron Smith, *Older Adults and Technology Use*, PewResearchCenter, http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use (Apr. 3, 2014).

4 Del. H. 345, 147th Gen. Assembly, http://www.legis.delaware.gov/LIS/lis147.nsf/vwLegislation/HB%20345/$file/legis.html (accessed

About the Authors

Suzanne Brown Walsh, JD, is a partner at Murtha Cullina LLP, a large regional law firm with multiple offices in Connecticut and Massachusetts. She holds a BS degree from Boston University and a JD from Suffolk University Law School. Ms. Walsh represents clients in the areas of estate and tax planning, estate and trust administration, trust and estate planning and administration for individuals with special needs, trust modifications, and trustee changes. She is a Connecticut Uniform Law Commissioner.

Catherine Anne Seal, CELA, CAP, is the senior member in the law firm of Kirtland & Seal LLC in Colorado Springs. Ms. Seal is the Public Administrator for the Fourth Judicial District of Colorado, serving El Paso and Teller Counties. She is the first person awarded an LLM degree in Elder Law from the Stetson University College of Law, graduating with honors. Ms. Seal received her BBA degree with honors from Colorado State University and a MS degree in marketing from the University of Colorado–Denver. She received her law degree from the University of Colorado Law School and holds a Graduate Certificate in Gerontology from the University of Colorado–Colorado Springs. She is a member of the American Bar Association's Real Property, Trusts and Estate Law Section where she serves as co-chair of the Surrogate Decision Making Committee. She is president of the National Academy of Elder Law Attorneys, and is past-chair of its Guardianship Section. She is the past-president of the Colorado Chapter of NAELA, and is one of only seven attorneys in Colorado designated a Certified Elder Law Attorney by the National Elder Law Foundation. As a member of the Colorado Bar Association, Ms. Seal is a past-chair of the Elder Law Section. She is the author of *Colorado Elder Law*, published by Thompson West Publishing.

lier state access laws, however, are much more limited.[5]

This article discusses the importance of fiduciary access to digital assets when an account holder becomes incapacitated or dies. It then discusses impediments to fiduciary access to digital assets, including the federal and state laws that protect these assets. Finally, the article describes the proposed statutory solution to access issues and suggests planning options to ensure fiduciary access to the digital assets of incapacitated or deceased individuals.

II. Lack of Access to Digital Assets

Digital assets are treated the same as nondigital assets in the majority of state probate statutes. This has proven unworkable, however, because the custodians of many online accounts have refused to recognize fiduciaries' authority over digital assets.[6]

Consider the case of John, a personal representative appointed under the will of his late brother-in-law, Stan, a widower who lived alone.[7] Stan and John had not kept in close touch during the last several years of Stan's life. Stan was computer savvy, embraced online banking, and set up a variety of automatic deposits and payments. His pension, Social Security, scheduled monthly withdrawals from his brokerage account, and distributions from his IRA were automatically deposited into his bank account. Stan did not receive paper statements from his bank, broker, or IRA custodian. Stan also paid his insurance premiums for his house, car, and health care out of his bank account by automatic payment as well as his mortgage, cable and internet, and utility bills. John found almost no documentation in Stan's home office regarding any of these items. If John had been granted access to Stan's email, John could have found out where Stan banked. Because John did not know where Stan banked and thus could not access Stan's account in a timely manner, the account balance was dissipated when the Social Security and pension deposits stopped, but the automatic payments continued until the account was overdrawn. As a result, Stan's mortgage and other bills became past due despite being legitimate expenses of estate administration. Allowing John to access Stan's email would have allowed him to locate Stan's bank, obtain statements, and determine what automatic deposits and automatic payments were being made to and from the account.

The Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA), which the Uniform Law Commission (ULC) approved on July 15, 2015,[8] gives fiduciaries limited, but much needed, access to digital assets, while taking into account the privacy and contractual rights of account holders and compliance with federal and state privacy laws.

III. Why Digital Access Is Important

Fiduciaries are responsible for handling

June 1, 2016).

5 Jim Lamm, *Delaware Enacts Fiduciary Access to Digital Assets Act*, Digital Passing, http://www.digitalpassing.com/2014/08/27/delaware-enacts-fiduciary-access-digital-assets-act (Aug. 27, 2014). This article also describes some state laws enacted before the Delaware law.

6 *See e.g. Ajemian v. Yahoo!, Inc.,* 987 N.E.2d 604, 614 (Mass. App. 2013).

7 This scenario is based on actual cases. The names are fictional and some facts have been changed for illustration purposes.

8 Natl. Conf. of Commrs. on Unif. St. Laws, Revised Uniform Fiduciary Access to Digital Assets Act (2015), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/2015_RUFADAA_Final%20Act_2015sep25.pdf (Sept. 25, 2015) [hereinafter Revised UFADAA].

an individual's finances. They have to inventory the person's assets and may need to manage or close the person's financial accounts or business; pay the person's debts, taxes, and expenses; and distribute the person's assets after death. Fiduciaries need access to the individual's digital assets to discharge their duties. Guardians for the incapable, in particular, may need to monitor social media and other online accounts for inappropriate posts and activity and prevent scam artists and cyber thieves from finding new prey.[9]

It is much more difficult to order prints of photographs, contact distant friends and family, collect travel rewards, book travel, or sort through financial records without access to email accounts. Most creditors and banks encourage customers to "go green" and receive bills and statements electronically. As medical providers transition to electronic medical records, pharmacy and medical records and histories are increasingly available to patients and caregivers via online systems. Elderly clients, similar to younger ones, often use online rental sites to rent their underused or unused vacation property to offset carrying costs.

Admittedly, younger people are more likely to own digital assets with significant monetary value. Digital currencies exist, such as Bitcoin.[10] Domain names continue to garner seven- and eight-figure sales prices. The highest price ever paid for a domain name was $36.5 million for Insurance.com in 2010.[11] Perhaps the most unusual valuable digital asset sold was a $635,000 virtual space station in Entropia Universe, an online gaming platform.[12]

A. Preventing Identity Theft

In 2014, $16 billion was stolen from 12.7 million identity fraud victims in the United States.[13] When an individual is unable to continue to monitor his or her online accounts because of incapacity or death, it becomes easier for criminals to hack these accounts, open new credit card accounts, apply for jobs, and even obtain state identification cards. Fiduciaries need to monitor and protect (perhaps by termination) online accounts.[14]

B. Consoling the Living

Stories abound of grieving family members and friends searching for answers, comfort, and support in the social media accounts, voicemails,[15] and other

9 *See Victims of Identity Theft,* Bureau of J. Statistics, 2014, http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf (Sept. 2015).

10 *See* Bitcoin, https://bitcoin.org/en, https://en.bitcoin.it/wiki/Introduction (accessed June 1, 2016); Joseph Wright, *Bitcoin Is Creating New Headaches for Estate Planners, Though It May Someday Cure Them*, Bloomberg BNA Elec. Com. & L. Rpt. (May 14, 2014); Denis T. Rice, *The Past and Future of Bitcoins in Worldwide Commerce*, Bus. L. Today (Nov. 2013).

11 Michael Berkens, *A New Domain Name Record? Quinstreet Acquisition of Insurance.com: $36.5 Million Dollars*, The Domains, http://www.thedomains.com/2010/08/09/a-new-domain-name-record-insurance-com-36-5-million-dollars (Aug. 9, 2010.

12 *See* Oliver Chiang, *Meet the Man Who Just Made a Half Million From the Sale of Virtual Property*, Forbes, http://www.forbes.com/sites/oliverchiang/2010/11/13/meet-the-man-who-just-made-a-cool-half-million-from-the-sale-of-virtual-property/#356b9d2e957e (Nov. 13, 2010).

13 Ins. Info. Inst., *Identity Theft and Cybercrime*, http://www.iii.org/fact-statistic/identity-theft-and-cybercrime (accessed June 1, 2016).

14 *See* Gerry W. Beyer & Naomi Cahn, *When You Pass On Don't Leave the Passwords Behind: Planning for Digital Assets*, 26 Prob. & Prop. 40 (2012).

15 Beth Teitell, *Preserving Voicemails Helps Modern Grieving Process*, Boston Globe, http://www.

digital assets of their deceased friends and relatives. Although the monetary value of social media accounts is generally small, access to these accounts may be priceless to family and friends.[16]

C. Marshaling Assets

Marshaling assets is a critical fiduciary duty, and it is impossible to manage a person's assets or estate until the assets are identified and collected. Marshaling traditional assets can be challenging. Fiduciaries acting on behalf of disorganized individuals who fail to plan, or simply keep poor records, have a difficult time identifying and collecting assets. However, when marshaling assets in digital accounts, such failures on the part of disorganized individuals can completely prevent, or at least delay, access to critical information and assets.

Consider the case of Bob, who was divorced from Sally, his second wife, several years ago. As part of the divorce decree, Bob was obligated to pay the mortgage on real property still owned in joint tenancy until his death, after which his estate would have no further obligation. Bob, who banked online, established automatic payment for the mortgage from his bank account. When Bob died, his brother, Bob's personal representative, could not locate information about the mortgage at Bob's home. After a 5-month exhaustive search, Bob's brother obtained a copy from the accountant of the previous year's IRS Form 1098 reporting the interest on the mortgage. Upon contacting the bank, Bob's brother was able to terminate the mortgage payments, but five payments had been made postmortem, contrary to the terms of the divorce decree. Sally refused to repay Bob's estate for the mortgage payments, claiming financial hardship. Bob's children from his first marriage threatened to sue Bob's brother for breach of fiduciary duty for failing to terminate the automatic payments immediately upon Bob's death.

Then there is the case of Ruth, who has dementia. Ruth's son, Jake, was appointed her conservator after her brokerage account was depleted from a balance of $300,000 to less than $100,000. When asked about the funds, Ruth said that she made some loans to her nephew and her grandson. When Jake asked Ruth if she had any paperwork about these transactions, she said that she corresponded with the nephew and grandson by email. Ruth had her broker transfer funds to her checking account and then withdrew cash, because her nephew and grandson requested cash. When asked about the loans, her nephew said that he asked Ruth for money and had received some gifts, but no loans, and her grandson denied requesting any money. Jake realized that without the email correspondence, he would have a difficult time proving that either the nephew or the grandson had even asked Ruth for money and that the emails might substantiate a claim that the money was loaned to each. Ruth could not remember her email user name or password or other information about the account.

IV. Impediments to Fiduciary Access to Digital Assets

Fiduciaries trying to access, collect, or manage digital assets face unique impediments that do not exist when dealing with traditional assets.

bostonglobe.com/lifestyle/style/2013/11/20/grief-has-modern-form-mourning-lost-voicemail-from-deceased-loved-one-surely/RQDlIvFuavZbzTxQEAiyiJ/story.html (Nov. 20, 2013).

16 Tracy Sears, *Family, Lawmakers Push for Facebook Changes Following Son's Suicide*, CBS 6 (WTVR-TV, Richmond, VA), http://wtvr.com/2013/01/08/legislation-introduced-for-access-to-deceased-persons-digital-property (updated Jan. 9, 2013).

A. Passwords and Encryption

Most online accounts are password protected, and the passwords can generally be reset only with access to the account holder's email account (if the accounts can be reset or recovered at all). 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, or when a software feature protects the data.

For example, Apple designed its iPhone iOS9 operating system with an auto-erase feature that prevents passcode-guessing. After 10 incorrect passcodes, the phone permanently destroys the data in the phone needed to decrypt the phone. As a result, the FBI reportedly paid over $1.3 million to a computer expert to access the San Bernardino shooter's iPhone 5C, after its auto erase passcode protection feature was enabled, encrypting its locally stored data.[17] As was widely reported at the time, before the FBI identified and paid its consultant that princely sum to hack into the phone, Apple was contesting a federal court order requiring that it assist the FBI in neutralizing this feature of its software.

The Apple encryption dispute in the San Bernardino case did not involve the Fourth Amendment or any federal privacy law (discussed in Sections C and D, below). Before it sought the court order against Apple, the federal government had obtained a search warrant, supported by probable cause. In addition, the phone was owned by the shooter's employer, which had consented to the FBI accessing the phone.[18] The problem of data inaccessibility was caused by the phone's software encryption features.

Regardless of where the public policy line is drawn in the law enforcement versus individual privacy debate, the privacy arguments seem to be driving technology companies, such as Apple, to increase their use of encryption to protect customers' phones and online accounts.[19] Rumor has it that Apple was working on enhanced iCloud security features, which would encrypt users' data with the passcodes of their devices, so that even Apple could not access user data or hand over the encryption keys to the government if it requested them. This could make it more difficult for Apple to help Apple customers retrieve data if they have forgotten the passcode, so it could backfire and alienate its customers.[20]

For this reason, it is vitally important to mention the importance of passcodes to clients with Apple devices and iCloud accounts.

B. Terms-of-Service Agreements

Even if the fiduciary can find a password, the account provider's terms-of-service agreement (TOSA) might forbid account access by anyone except the account holder[21]—implicitly barring a fidu-

17 Julia Edwards, *FBI paid more than $1.3 million to break into San Bernardino iPhone,* Reuters, http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB, (accessed July 19, 2016).

18 Jeff Kosseff, *In The Apple Encryption Debate, Can We Just Have The Facts Please?*, https://techcrunch.com/2016/02/25/in-the-apple-encryption-debate-can-we-just-have-the-facts-please/ (accessed July 19, 2016).

19 Benjamin Mayo, *Apple Working on Stronger iCloud backup encryption and iPhone security to counter FBI unlock requests*, http://9to5mac.com/2016/02/25/apple-working-on-stronger-icloud-backup-encryption-and-iphone-security-to-counter-fbi-unlock-requests/ (accessed July 19, 2016).

20 *Id.*

21 Yahoo!, *Yahoo Terms of Service*, http://info.ya

ciary from access. Online TOSAs are frequently silent about postmortem options and often simply prohibit postmortem transfer.[22]

Fiduciaries have been forced to challenge TOSAs. The Massachusetts appellate 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 his estate, sought access to John's Yahoo account to console grievers and to collect estate assets.[23] Yahoo refused access to the account even though the surviving brother had opened and originally shared access to it; he had, however, subsequently forgotten the password.[24] Yahoo attempted to dismiss the Massachusetts declaratory action based on the California forum designation provision; it also claimed that the emails were not 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. In its opinion, the court discussed the differences between "clickwrap" agreements (which require users to click an "I agree" box) and "browsewrap" agreements (to which users impliedly agree to the posted terms by accessing the website or page or by some other action but need not expressly agree to the terms).[25] The court concluded that without evidence that the account holder had agreed to the TOSA, it was not enforceable. It also concluded that the estate's co-administrators were not parties to the TOSA and thus could not be bound by it. Nonetheless, the appellate court did not order Yahoo to provide access to the account; instead, it remanded the case to the probate court to determine whether the emails were an asset of the estate and whether federal laws permitted Yahoo to disclose them. Therefore, even though restrictive TOSAs will not necessarily preclude fiduciary access, fiduciary access cannot be presumed.

C. Federal and State Computer Fraud and Abuse Acts

The Federal Computer Fraud and Abuse Act (CFAA) criminalizes 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 … shall be punished as provided in subsection (c) of this section.[26]

This criminalizes two kinds of computer trespass: access "without authorization" and access that "exceeds authorized access." The CFAA defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[27] A related provision

hoo.com/legal/us/yahoo/utos/terms (updated Mar. 16, 2012). "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 … ."

22 The TOSAs of various companies appear at Mylennium Digital Executor Servs., *Domain Information Resources*, https://www.mylennium.com/domaininfo (accessed June 1, 2016).

23 *Ajemian*, 987 N.E.2d at 614.

24 *Id.*

25 *See generally* Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 Bus. Law. 279, 291 (2003); *see also* Cahn et al., *supra* n. 1.

26 18 U.S.C. § 1030(a)(2)(C)(2012) (emphasis added).

27 *Id.* at § 1030(e)(6).

of the statute criminalizes the same acts, but additionally requires knowledge and intent to defraud.[28]

Unauthorized use includes "obtain[ing] … information" (such as by accessing emails or internet accounts) from a "protected computer," which is defined as any computer connected to a government or financial institution as well as one "used in or affecting interstate or foreign commerce or communication."[29] Because most internet servers are not located in the same state as a website's users, internet use almost always involves obtaining information from a protected computer and therefore implicates the CFAA.[30] The term "computer" includes desktop computers, laptops, notepads, tablets, and smartphones.[31]

Every state has an analogous statute, which varies in coverage, but typically prohibits unauthorized access to computers.[32]

Even though a fiduciary is authorized by the account holder or state law to use a computer or to act on behalf of an account holder, the fiduciary is not necessarily exempt from CFAA prosecution.[33] There is no question that a fiduciary is authorized, in the normal sense of the word, to access an account holder's computer or system that the fiduciary lawfully possesses, controls, or owns by virtue of the proscribed authority of a fiduciary. The analogy is 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 technically different from accessing the account holder's digital accounts or assets, which are stored on the provider's server, not the user's. 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.[34]

As we know, few people read TOSAs. Most of us open accounts and click our agreement to the TOSAs without even a cursory glance. To illustrate how easy it is to unintentionally violate a TOSA, *The Guardian* newspaper reported in 2014 that six users of a free Wi-Fi hotspot in the United Kingdom agreed to sell their firstborn children to the devil.[35] Because the CFAA defines a "protected computer" as one affected by or involved in interstate commerce — effectively all computers with internet access — a prosecutor's broad interpretation of "exceeds authorized access" would make every violation of a TOSA a federal crime. Put differently, criminalizing a simple TOSA violation would make criminals out of virtually everyone who uses any internet-enabled device, because:

28 Id. at § 1030(a)(4); this is the "second prong" of the CFAA.

29 *Id.* at § 1030(e)(2).

30 *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

31 *U.S. v. Mitra,* 405 F.3d 492, 495–496 (7th Cir. 2005).

32 Natl. Conf. of St. Legislatures, *Computer Crime Statutes*, www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (as of May 12, 2016).

33 *See* James D. Lamm et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries From Managing Digital Property*, 68 U. Miami L. Rev. 385, 399–401 (2014).

34 Cahn, *supra* n. 1, at 10.

35 Tom Fox-Brewster, *Londoners Give Up Eldest Children in Public Wi-Fi Security Horror Show,* The Guardian, http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause (Sept. 29, 2014).

> The Internet is a means for communicating via computers: Whenever we access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube and do the thousands of other things we routinely do online, we are using one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.[36]

The problem is that (some would say) overzealous federal prosecutors are using the CFAA to prosecute defendants based solely on violations of a website's TOSA.[37] While they have not prosecuted any fiduciaries, friends, or spouses for password sharing done without any intent to violate a TOSA or employer policy, there is nothing in the statute, if it is interpreted expansively, that prohibits the government from doing so.[38]

The United States Court of Appeals for the Ninth Circuit has decided several cases involving the scope of the "unauthorized access" that is criminalized under the CFAA, and the legal rationales for the decisions are not entirely consistent. The first is commonly known as *Nosal I,* involving an employee (Nosal) of an executive search firm who left the firm to start a competing business. He thereafter convinced his former coworkers to use their account credentials to download information for him from a confidential database on the former employer's computer system. The coworkers were authorized to access the former employer's database, but company policy forbade disclosure of confidential information.[39]

The government initially charged Nosal with violating the second prong of the CFAA[40] and aiding and abetting his former coworkers (who exceeded [their] authorized access with intent to defraud) when they violated the employer's terms of use by accessing the employer's network for non-work purposes. Nosal filed a motion to dismiss the indictment, arguing that the CFAA targeted hacking, not misuse of information obtained with permission.[41] The Ninth Circuit agreed with him, and ruled that simply violating the TOSA did not and should not "exceed authorized access" under the CFAA.[42]

> Sitting *en banc*, the court narrowly construed the CFAA to avoid criminalizing technical TOSA violations: "[W]e hold that the phrase "exceeds authorized access" in the CFAA does not ex-

36 676 F.3d at 861.

37 *See United States v. Nosal,* D.C. No. 3:08-cr-00237-EMC-1, 9th Circuit Court of Appeals, July 5, 2016; *See also* Andrea Peterson, *The Law Used to Prosecute Aaron Swartz Remains Unchanged a Year After His Death*, Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2014/01/11/the-law-used-to-prosecute-aaron-swartz-remains-unchanged-a-year-after-his-death (Jan. 11, 2014).

38 *See* Justice Reinhardt's dissenting opinion in *Nosal II, supra* n. 37.

39 *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012)(en banc).

40 18 U.S.C. §1030(a)(4).

41 *See* "Statutory Interpretation — Computer Fraud And Abuse Act — Ninth Circuit Holds That Employees' Un-Authorized Use of Accessible Information Did Not Violate the CFAA." *United States v. Nosal*, 676 F. 3d 854 (9th Cir. 2012)(en banc).

42 *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012)(en banc); *see also United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015), reaching a similar result.

> tend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly."[43]

Thus, employees do not "exceed authorized access" if they access a company computer in a manner that violates the company's computer use policies, as long as they are authorized to access the computer.[44]

Unfortunately, subsequent decisions in the Ninth and other circuits more broadly construed the CFAA,[45] and the CFAA decisions among the various circuits conflict.[46] In the Ninth Circuit, the government ultimately reindicted Nosal, using a new theory. This time, the prosecution argued that after Nosal and his colleagues left the company, they had no underlying legal right to access the company's computer network at all. Because they lacked any legal rights to access the network, their use of a sympathetic current employee's login credentials violated the first (and broader) prong[47] of the CFAA's ban on "access without authorization."[48] This theory worked, and Nosal was convicted for accessing a protected computer "without authorization" under the first prong of the CFAA, and thereafter a divided panel of the Ninth Circuit upheld (by a 2-1 vote) his conviction in *Nosal II*.[49] The majority decided that Nosal could be convicted for accessing his former employer's computer "without authorization" because the employer had revoked his credentials, and he nevertheless used the system through and with the permission of a sympathetic, still credentialed co-worker.

This is not a comforting rationale, because TOSA's routinely prohibit password sharing and other third-party access.[50] It can also be difficult to know when access that is technologically possible is not authorized by a TOSA.

The effect of the court's *Nosal II* decision broadly construing the CFAA is somewhat ameliorated by its subsequent holding that a person who visits a website after being expressly and directly told not to do so by its owner could be committing a federal crime under the CFAA.[51] In that case, known as "Power Ventures," the court held that after Facebook sent a company called Power Ventures a cease and desist letter demanding it stop accessing Facebook's service and violating its TOSA by doing so, the company violated the CFAA by continuing to access Facebook's

43 *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012) (en banc).

44 *Id,* at 863.

45 Andrew Trombly, *Right for the Wrong Reasons: The Ninth Circuit Excludes Misappropriation from the CFAA's Ambit in* United States v. Nosal, 54 B.C. L. Rev. (2013), http://lawdigitalcommons.bc.edu/bclr/vol54/iss6/11(visited Aug. 4, 2016).

46 *Compare e.g., United States v. John,* 597 F.3d 263 (5th Cir. 2010), *United States v. Rodriguez*, 628 F.3d 577(11th Cir. 2010), finding that a use violation itself was not a crime under the CFAA, and *Nosal I,* 676 F.3d 854 and *United States v. Valle,* 807 F.3d 508 (2nd Cir. 2015) in which the Ninth and Second Circuits held that it was not.

47 18 U.S.C. Section 1030(a)(2).

48 *United States v. Nosal,* D.C. No. 3:08-cr-00237-EMC-1, 9th Circuit Court of Appeals, July 5, 2016.

49 *Id.*

50 *See* amicus brief filed by the Electronic Frontier Foundation for a good synopsis of the policy arguments against broadly construing the CFAA in this manner, https://www.eff.org/document/eff-amicus-brief-2014 (accessed July 22, 2016).

51 *Facebook v. Vachani,* No. 13-17102, D.C. No.5:08-cv-05780-LHK, 9th Circuit Court of Appeals, July 12, 2016.

service.[52] The decision suggests that a visitor must be told by its owner to stay off the website and the owner's servers before the visitor violates the CFAA by visiting it anyhow. The problem with that result is that there is not much of a difference between visiting an online account with the account holder's permission and password, knowing that access is not permitted by the company, and visiting the site after the company directly tells the visitor not to do so.[53]

As a result, it is not at all clear whether or not a simple password sharing violation of an online account TOSA is a crime under the CFAA. Professor Orin Kerr of GWU Law School has helpfully proposed the use of an "authentication-based" approach for shared password cases to identify CFAA violations that will lead to prosecution or damages.[54] He proposes that the analysis of shared password and business access cases should be based on the delegation of authority by authenticated accounts and their users. When a computer owner (such as a business) gives a user (an employee or manager) an account, the computer owner delegates to the account holder and her agent the rights to access the account. If and when the computer owner thereafter revokes the account, it cancels the user's rights to access and use the account.[55]

If courts adopt Kerr's rationale, whether a person's use of a shared password violates the CFAA will depend on whether the user intentionally acted outside the agency of the legitimate account holder. If the user, in so acting, accesses the account in a manner consistent with and within the agency relationship, that use would not violate the CFAA. If the user acted outside the agency relationship, that would be an actionable CFAA violation.[56] So, it would be okay for a fiduciary to use a password to terminate a decedent's iTunes account and remove the deceased holder's credit card on file, but not to use the credentials to download the music and movie files for the fiduciary's personal use. By analogy to a more traditional situation, the permissible use would be a person using a key (password) to enter their neighbor's house and feed the dog, which becomes an actionable trespass (CFAA violation) when the person stays in the house and begins rifling through the owner's desk to snoop, after feeding the dog.[57]

This analysis, if embraced consistently by courts and applied to fiduciaries, would not make a fiduciary's access to an account with a principal's, settlor's, incapable person's, or decedent's permission or password a criminal CFAA violation, as long as the fiduciary acted in the same manner as the legitimate, original account holder and *otherwise* adheres to the TOSA.

Until Congress amends and clarifies the CFAA, the scope and breadth of the CFAA's reach will remain unclear, including its impact on fiduciaries trying to perform their statutory duties. That lack of clarity will continue to have a chilling ef-

52 *Id.*

53 Orin Kerr, *9th Circuit: It's a federal crime to visit a website after being told not to visit it,* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/12/9th-circuit-its-a-federal-crime-to-visit-a-website-after-being-told-not-to-visit-it/ (July 12, 2016).

54 Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016).

55 Orin Kerr, *Password-sharing case divides Ninth Circuit in Nosal II,* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/06/password-sharing-case-divides-ninth-circuit-in-nosal-ii/ (July 6, 2016).

56 *Id.*

57 *Id.*

fect on fiduciaries as they attempt to deal with the digital assets of account holders.

D. The Stored Communications Act

The Fourth Amendment to the U.S. Constitution provides citizens with a strong expectation of privacy in their homes. As a result, the government usually cannot search our homes without first showing probable cause and obtaining a warrant authorizing a search.

When we use a computer network, we may have the same expectation of privacy; however, because the network is not physically located or even being accessed in our computers or in our homes, it is outside the coverage of the Fourth Amendment.[58] To fill that gap, in 1986 Congress enacted the Stored Communications Act (SCA) as a part of the Electronic Communications Privacy Act (ECPA)[59] to respond to concerns that internet privacy poses new dilemmas with respect to application of the Fourth Amendment's privacy protections. The SCA prohibits certain providers of *public* electronic communications services from disclosing the *content* of its users' communications to a government or nongovernment entity (different rules apply to each) except under limited circumstances that are akin to the warrant required under the Fourth Amendment.[60] The SCA 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 content of any electronic communications in the absence of an applicable exception, such as consent by the account holder.[61]

Providers are permitted, but not required, to divulge noncontent, such as the user's name, address, connection records, IP address, and account information to a nongovernmental entity.[62] The subject line of an email has been held to be content protected by the SCA.[63]

Second, the SCA establishes limits on the provider's ability to voluntarily disclose to the government or any other person or entity the content of communications.[64] All private social media account

58 *See generally* 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).

59 Pub. L. No. 99-508, 100 Stat. 1848 (1986). The ECPA is codified at 18 U.S.C. §§ 2510–2522. The SCA is codified at 18 U.S.C. §§ 27012711.

60 *See generally* Kerr, *supra* n. 58, at 1214.

61 18 U.S.C. § 2702(a)(1) prohibits voluntary disclosure of the content of an electronic communication to anyone, whereas 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 some exceptions exist in the case of an emergency. 18 U.S.C. § 2702(b).

62 *Id.* at § 2702(c)(6).

63 *Optiver Austrl. Pty. Ltd. v. Tibra Trading Pty. Ltd.,* Case No. C 12-80242 EJD (PSG), 2013 U.S. Dist. Lexis 9287 (N.D. Cal. Jan. 23, 2013).

64 *See* Kerr, *supra* n. 58, at 1212–1213 ("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 providers did not want to disclose some information, and the National Security Agency either coerced them to disclose the information or simply took the information without their knowledge. *See e.g.* Ryan Lizza, *The Metadata Program in Eleven Documents*, New Yorker, http://perma.cc/ 8R7Y-GBAE (Dec. 31, 2013); Ryan Lizza, *State of Decep-*

content (e.g., photos, videos, posts) is protected by the SCA.[65]

A provider of public electronic communications services can *voluntarily* disclose the content of communications, but only if an *exception* to the SCA's blanket prohibition against disclosure applies.[66] The relevant exception for fiduciaries permits a provider to disclose communication content if the provider has the "lawful consent" of "the originator," an addressee or intended recipient of the communications, or the subscriber.[67] There is evidence that Congress intended authorized agents to be able to authorize disclosure of the contents of electronic communications.[68] However, some providers refuse to give executors access to the content of decedents' email 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 motion to quash a civil subpoena for content 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.[69] The court granted Facebook's motion to quash the subpoena but refused to address whether Facebook could voluntarily disclose the content.[70]

While not as troubling as the possibility of criminal prosecution, fiduciaries who violate TOSA's, even by using a password with permission, could still face civil fines under the SCA. 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 email 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 her later access was unauthorized under the SCA. Despite very thin (or nonexistent) testimony to support the damage claim, the jury awarded the plaintiff $450,000 for the unauthorized intrusion.[71]

Recently, however, after a Florida jury decided *against* a damages award for a similar violation, a Florida federal appeals court held that statutory damages under the SCA may not be awarded absent evidence of actual damages.[72]

E. Heightened Privacy Concerns

Electronic communications and ac-

tion: Why Won't the President Rein in the Intelligence Community? New Yorker, http://perma.cc/ F4KK-FVXG (Dec. 16, 2013); Laura W. Murphy, *The NSA's Winter of Discontent*, Huffington Post, http://perma.cc/3V8U-6X6W (updated Feb. 11, 2014).

65 *See* Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1267–1278 (2012).

66 18 U.S.C. § 2702(b).

67 *Id.* at § 2702(b)(3).

68 Senate Report No. 99-541 on ECPA, at page 37, which says: "Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication."

69 *In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things*, Order Granting Facebook, Inc.'s Motion to Quash, (N.D. Cal. Sept. 20, 2012) (No. C 1280171 LHK (PSG)).

70 *Id.*

71 Jury Verdict Form at 1–3, *Cheng v. Romo,* No. 11-cv-10007-DJC, 2013 WL 2245312 (D. Mass. Apr. 29, 2013); *Cheng v. Romo*, 2012 WL 6021369, at *1–3 (D. Mass. Nov. 28, 2012).

72 *Vista Marketing, LLC v Burkett*, 812 F.3d 954, 975 (11th Cir. 2016).

counts are unlike traditional communications and accounts in several ways. Unlike paper communications, lost and even deleted emails might be easily located and retrieved from an email service provider. Access to a decedent's emails might be important, perhaps for sentimental value, but more likely because the decedent's email account contains the information necessary to continue a business or collect other assets. A decedent or incapable person might have opened an online account (e.g., to access embarrassing content or a dating service such as Ashley Madison) with the expectation that the account would remain private and undiscoverable by anyone, including a fiduciary. Without evidence of the account holder's intent, it is impossible to show that the user intended the account to be accessible to others and not private.

V. Online Tools

Had company founders contemplated incapacity and death when they created various social media and other products, they presumably would have created online tools and account settings to address those eventualities.

In April 2013, Google was the first major technology firm to offer such an online tool, which it calls Inactive Account Manager.[73] This tool allows users to determine (within preset options) what will happen to their Google accounts after a predetermined period of inactivity. A user can set the period of inactivity that triggers a Google notification, and Google will alert the user by text and email 1 month before deleting the user's account. A user can direct Google to notify up to 10 "beneficiaries" that the account will be deleted. After these beneficiaries are notified, they can download the user's Google content (e.g., Gmail, photos, videos, blogs). Alternatively, the user can simply instruct Google to delete all account content.[74] This feature will not assist with postmortem account access if the account holder did not use it or if a designated beneficiary is unavailable, incapable, dead, or declines to share information with the fiduciary.

To address these deficiencies, in August 2015, Google updated its support policy on postmortem access.[75] The updated policy now indicates that "immediate family members and representatives" seeking to obtain content from an account may provide the name of the deceased user and other information to Google for review. Such persons will have to upload proof, such as an obituary or testamentary letters, to obtain the content: They will not be given access to the account itself. Google's new policy on postmortem access to accounts of users who did not use its online tool is similar to Facebook's.

In early 2015, Facebook updated its policy on postmortem account use and access, providing for the designation of a "legacy contact."[76] Previously, once a deceased user's account was "memorialized,"[77] Facebook would not al-

73 Google, *About Inactive Account Manager,* https://support.google.com/accounts/answer/3036546?hl=en (accessed June 1, 2016).

74 *Id.*

75 Google, *Submit a Request Regarding a Deceased User's Account,* https://support.google.com/accounts/contact/deceased?hl=en (accessed June 2, 2016).

76 Facebook Help Ctr., *What Is a Legacy Contact?* https://www.facebook.com/help/1568013990080948 (accessed June 2, 2016).

77 When a user account has been memorialized, sensitive information (e.g., phone numbers) is removed and the account will no longer generate reminders of the deceased user's birthday. The deceased user's profile will no longer be visible to anyone except a confirmed friend;

low anyone except the user (who presumably would have to prove that he or she did not actually die) to log into it. It did, however, allow verified family members to request that the account be removed from Facebook. The new Legacy Contact feature provides that after an account is memorialized, the designated legacy contact can write a pinned post for the user's profile, respond to new friend requests, and update the user's profile picture and cover photo. The legacy contact *cannot* log into the account; remove or change previous posts, photos, or other things shared on a timeline; read messages sent to other friends; or remove any friends.[78] However, Facebook may allow an authorized representative (e.g., a family member) to obtain content "in response to a valid will or other legal consent document expressing clear consent."[79] It may still allow an authorized representative to obtain content with a court order via a special request.[80]

nonfriends will no longer be able to find the profile in search queries either. Confirmed friends of the deceased user can continue to leave "wall" posts in remembrance on the user's timeline. Facebook Help Ctr., *What Will Happen to My Account If I Pass Away?* https://www.facebook.com/help/103897939701143 (accessed June 2, 2016); Caroline McCarthy, *With 'Memorialized' Profiles, Facebook Sees Dead People,* CNET, http://www.cnet.com/news/with-memorialized-profiles-facebook-sees-dead-people (Oct. 26, 2009).

78 Facebook Help Ctr., *supra* n. 76.

79 Facebook Help Ctr., *What Data Can a Legacy Contact Download?* https://www.facebook.com/help/408044339354739 (accessed June 2, 2016).

80 Facebook Help Ctr., *How Do I Request Content From the Account of a Deceased Person?* https://www.facebook.com/help/123355624495297?sr=13&query=special%20request&sid=2AW8JGwE2Kab8NawQ; *Special Request for Deceased Person's Account,* https://www.facebook.com/help/contact/228813257197480 (accessed June 2, 2016).

VI. Revised UFADAA

To ensure that fiduciaries can access digital assets, the ULC drafted the original UFADAA, which it approved in July 2014.[81] Its premise was that asset neutrality was needed to ensure that fiduciaries could access digital assets to the same extent and as easily as other intangible assets and tangible assets. The original UFADAA sought 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 by default.

Although the original UFADAA was drafted with the assistance of participating observers from Facebook, Google, Yahoo, NetChoice, Microsoft, and representatives from the gaming industry, technology industry opposition remained. The technology industry's primary objection to fiduciary access was the account holder's loss of privacy.[82] For example, Yahoo 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.[83]

81 Unif. L. Commn., *Uniform Fiduciary Access to Digital Assets Act (2014).*

82 Ltr. from AOL. et al. to Del. Gov. Jack Markell, *RE: Veto Request of HB 345, An Act to Amend Title 12 of the Delaware Code Relating to Fiduciary Access to Digital Assets and Digital Accounts* (July 8, 2014), http://netchoice.org/wp-content/uploads/Industry-Veto-Request-of-DE-HB-345-Signed.pdf.

83 Bill Ashworth, *Your Digital Will: Your Choice* Yahoo! Global Public Policy, http://yahoopolicy.tumblr.com/post/97570901633/your-digital-will-your-choice (Sept. 15, 2014).

Internet industry representatives also argued that the SCA requires the account holder's *express* consent to disclosure and that the account holder's "constructive consent" is insufficient.[84] The original UFADAA was premised on the notion that the fiduciary has the account holder's implied consent and does not need actual consent, which proved to be a substantial obstacle during enactment efforts. The technology companies also objected to UFADAA's override of their TOSAs and the administrative burdens it would impose on them. Finally, they cited consumer demand for private, encrypted, anonymous services. Privately, they expressed concern that offering postmortem access options during sign-up would scare away new customers.[85]

During the first legislative sessions after the original UFADAA was approved, industry opposition to each state bill grew louder and opposing lobbyists became more numerous. After 9 months of increasingly difficult legislative battles, the ULC and technology industry representatives met and negotiated a compromise — Revised UFADAA, which reorganized the original act and revised almost all of its provisions. While it retains the original UFADAA's comprehensive scope and applies to personal representatives, conservators, agents, and trustees, Revised UFADAA also contains some of the provisions of the restrictive industry bill known as the Privacy Expectation Afterlife and Choices Act (PEAC).[86] As a result, Facebook and Google support the revised act, as do the American Civil Liberties Union and the Center for Democracy & Technology.[87] The online company and business companies' trade association NetChoice has some excellent materials which endorse Revised UFADAA on its website as well.[88] As of July 26, 2016, Revised UFADAA had been enacted in 18 states, and was pending in several others.[89]

A. Key Concepts and Definitions

Revised UFADAA covers personal representatives, conservators, agents acting under powers of attorney, and trustees.[90] It defines "online tool" as an electronic service that allows a user, in an agreement distinct from the TOSA, to provide directions for the disclosure or nondisclosure of digital assets to a third person.[91] That third person can be a fiduciary or a "designated

84 *Negro v. Super. Ct.,* 2014 WL 5341926 (Cal. App. 4th Dist. 2014).

85 Sen. Jud. Comm., *Regarding SB 518, An Act to Amend Title 20—Fiduciary Access to Digital Assets,* 114th Cong. (June 16, 2015), https://netchoice.org/wp-content/uploads/Joint-testimony-PA-SB-518-and-PEAC.pdf (joint testimony of William Ashworth, Yahoo; Daniel Sachs, Facebook; and Steve DelBianco, NetChoice).

86 NetChoice, *Privacy Expectation Afterlife and Choices Act (PEAC),* https://netchoice.org/library/privacy-expectation-afterlife-choices-act-peac/ (accessed July 26, 2016).

87 Facebook and Google's endorsements are part of an enactment kit available for download. Unif. L. Commn., *Acts: Fiduciary Access to Digital Assets Act,* Revised (2015), http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20 (accessed Aug. 2, 2016). Click on "Download an Enactment Kit" under "Legislation Information Kit" (accessed June 2, 2016).

88 NetChoice, *supra* n. 86.

89 Univ. L. Commn., *Legislative Fact Sheet — Fiduciary Access to Digital Assets Act,* Revised (2015), http://tinyurl.com/hgvgnln (accessed July 26, 2016). The enacting states are: Arizona, Colorado, Connecticut, Florida, Hawaii, Idaho, Indiana, Maryland, Michigan, Minnesota, Nebraska, North Carolina, Oregon, South Carolina, Tennessee, Washington, Wisconsin, Wyoming.

90 Revised UFADAA, *supra* n. 8.

91 *Id.* at §§ 2(16), 4.

recipient" who need not be a fiduciary. A "digital asset" is defined as "an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record."[92] This includes both the catalog, or log, of electronic communications and the content of the communications but not securities or traditional currency.[93] For example, neither a security held in street name nor money in a bank is considered a digital asset. Revised UFADAA simply addresses the fiduciary's right to access all relevant electronic communications and the online account that provides evidence of ownership.

B. Disclosure

The original UFADAA provided most fiduciaries with default authority over access to information protected by federal privacy laws. Revised UFADAA Section 4 instead provides that users, either in an online tool or in a record (i.e., a will, power of attorney, or trust instrument), may consent to disclosure of protected electronic communications content. Such express consent overrides a TOSA's boilerplate prohibition against access or disclosure. Without express consent, Revised UFADAA does not require custodians to disclose user content.

The Revised UFADAA's hierarchy for determining disclosure is as follows:

1. Online tool directions, if an online tool is offered and modifiable

2. Directions in a will, trust, power of attorney, or other record

3. TOSA provisions (which govern access to accounts of users who did not plan for third-party access to their online accounts and digital assets)

Revised UFADAA Section 5 expressly preserves the custodian's TOSA except as necessary to effectuate a user's express consent to disclosure under Section 4.

Revised UFADAA Section 6 allows the custodian to determine whether to grant the fiduciary full access to an account, or partial access sufficient to perform the fiduciary's duties, or to provide a "data dump" in digital or paper form of whatever assets the user could have accessed. Deleted assets are not included, and the custodian may charge a reasonable fee for the access or disclosure. Revised UFADAA also contains provisions protecting custodians from unduly burdensome requests.

C. Access by Various Parties

1. Personal Representatives

Revised UFADAA Section 7 gives a personal representative limited access to a decedent's digital assets. The personal representative must demonstrate that the decedent expressly consented to the disclosure of protected content, or the court can direct disclosure if the personal representative provides a written request, a death certificate, a certified copy of the letter of appointment, and evidence of the disclosure consent. The personal representative must also provide, on request, information that identifies the account and links the decedent to it, which may include a court order. Revised UFADAA Section 8 requires disclosure of all other digital assets, unless prohibited by the decedent or directed by the court, once the personal representative provides the requisite verifications. Thus, Section 8 is intended to give personal representatives default access to the catalog of electronic communications and other digital assets not protected by federal privacy laws.

92 *Id.* at § 2(10).

93 *Id.* at § 2cmts.

2. Conservators (Including Guardians)

Conservator authority over assets in online accounts is more limited under Revised UFADAA. Section 14 permits a court to authorize conservator access to digital assets after the opportunity for a hearing. It does not permit a conservator to request that a custodian disclose a protected person's electronic communications content simply by virtue of the conservator's appointment. Under Section 14(b), the custodian may be required to disclose noncontent if the conservator obtains a court order and provides the necessary verifications. Section 14(c) permits a conservator with plenary authority to ask the custodian to suspend or terminate the protected person's account for good cause. This allows a guardian or conservator who becomes concerned about an incapable person's online behavior to request suspension or termination of a social media account. However, Section 14 will not allow the conservator or guardian, even with a court order, to monitor the account for signs of trouble. The fiduciary's only option is to threaten account termination or suspension to persuade the incapable person to allow the fiduciary to access and monitor the account.

3. Agents Acting Under Powers of Attorney

Similar to the original UFADAA, Section 9 of Revised UFADAA provides that an agent has authority over a principal's electronic communications content only if the principal expressly grants that authority. Thus, access to electronic communications content by an agent is a "hot" power (i.e., it has to be specifically granted by the principal). Section 10 requires disclosure of all other digital assets to an agent with specific digital asset authority or general authority, with the requisite verifications that protect against disclosure of another person's account content.

4. Trustees

Revised UFADAA Section 11 comment states, "Section 11 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." The Section 11 comment states, "For accounts that are transferred into a trust by the settlor or in another manner, a trustee is not the original account holder of the account, and the trustee's authority is qualified. Thus, Section 12, governing disclosure of content of electronic communications from those accounts, requires the account holder's consent." Section 13, governing disclosure of all other digital assets, does not. Access and transfer of the digital assets into a trust would be accomplished by the settlor (while 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 when drafting trustee power provisions.

D. Fiduciary Duty and Authority

Revised UFADAA Section 15 specifies the nature, extent, and limitations of the fiduciary's authority over digital assets. Subsection (a) imposes fiduciary duties such as care, loyalty, and confidentiality. Subsection (b) subjects a fiduciary's authority over digital assets to the TOSA, except to the extent the TOSA is overridden by an action taken pursuant to Section 4, and it reinforces the applicability of copyright and fiduciary duties. Finally, subsec-

tion (b) prohibits a fiduciary's authority from being used to impersonate a user. Section 15(c) permits the fiduciary to access all digital assets not in an account or subject to a TOSA. Section 15(d) further specifies that the fiduciary is an authorized user under any applicable law on unauthorized computer access. Section 15(e) clarifies that the fiduciary is authorized to access digital assets stored on devices, such as computers and smartphones, without violating state or federal laws on unauthorized computer access.

Section 15(f) gives the fiduciary the option of requesting that an account be terminated if termination would not violate a fiduciary duty. Therefore, if the fiduciary wanted to terminate an online storage account because it held valuable photographs that embarrassed the fiduciary, but the fiduciary knew that the account holder wanted to maintain the photographs, termination could violate the fiduciary duties of loyalty and good faith.

E. Custodian Compliance and Immunity

If a fiduciary has access under Revised UFADAA and properly substantiates his or her authority, a custodian must comply with the fiduciary's request for asset disclosure or account termination within 60 days of receipt of all required documentation. If the custodian does not comply, the fiduciary may apply for a court order directing compliance, which must contain requisite findings of fact. Section 16(c) gives a custodian the right to notify a user that the fiduciary has requested disclosure or termination, and Section 16(d) allows the custodian to deny the request if the custodian is aware of lawful access to the account after the request was made. Custodians insisted on this to protect joint account holders and businesses against denial of access to joint accounts.[94] Finally, Section 16(e) gives custodians the right to obtain or to require fiduciaries to obtain court orders that make factual findings relevant to the request. The latter provision was negotiated in response to industry insistence that agents and trustees *always* be required to obtain court orders, which was not acceptable to the drafting committee.[95] In exchange, Section 16(f) immunizes a custodian who complies with a request under the Act.

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 precludes fiduciary access to employer-provided email systems and data. By implication, it allows fiduciaries to access employees' personal accounts that are not used for business. For example, a Google employee's fiduciary would not have access to the employee's business email or other business accounts but could access the employee's personal Gmail account.

VII. The Importance of Planning

Revised UFADAA's limited default authority over electronic communications content will penalize those who fail to plan for third-party access to their online accounts and digital assets. Likewise, advisors who fail to discuss digital assets and access with their clients will be hard-pressed to explain that oversight. At a

94 Based on notes of the Uniform Law Commission May 2015 meeting with industry representatives (on file with co-author Suzanne Brown Walsh).

95 Based on co-author Suzanne Brown Walsh and committee member Turney P. Berry's conversations with Daniel Sachs, the technology industry's point person during negotiations (notes on file with co-author Suzanne Brown Walsh).

minimum, practitioners should ask clients about email accounts and digital assets and ensure that fiduciaries are given appropriate and express powers in all wills, trusts, and powers of attorney. Further, when drafting fiduciary power provisions, successors and the application of the authority over digital accounts to successors should be considered. The client may be comfortable with the first named fiduciary having access to accounts but may not want co-fiduciaries or successors to have the same access. Finally, assuming that more companies eventually offer online tools, it will become important to coordinate the designations made in those tools with the provisions of the client's estate plan (just as beneficiary designations are coordinated with the client's estate plan).

VIII. Conclusion

One of the consequences of our clients' need for data protection and their desire for privacy is the potential for economic loss during incapacity or the potential for economic loss to their beneficiaries after death. In the case of digital assets, ineffective or inadequate planning can cause irreparable economic harm because fiduciaries and family members may be denied access—at least to protected electronic communications content. Even though Revised UFADAA will allow some fiduciary access, it will not and cannot serve as a substitute for thoughtful planning.