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

By Suzanne Brown Walsh

Introduction. In the past, fiduciaries could easily identify, marshal, collect, and manage assets. Often, the biggest nuisance was convincing a recalcitrant financial institution to honor a power of attorney, and personal representatives and conservators, appointed by courts, encountered few problems. That landscape changed forever with the advent and popularity of digital assets and accounts.

Today, individuals may own digital assets and accounts with significant monetary value, such as cryptocurrency.[1] Even items of sentimental value are digital today. Executors who need to access photos, contact friends and family or sort through correspondence may find that impossible without access to email and online storage accounts. Guardians for the incapable 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.[2]

Despite the importance of access to digital assets, clients are often unaware that passwords and encryption can completely prevent fiduciary access to assets and data. According to a 2017 study, between 30 to 50 percent of all Bitcoin will likely be lost and out of circulation -- totaling $20 billion in value -- due to private key loss.[3]

Absent express instructions from the account holder, online custodians routinely deny fiduciaries access to a decedent's electronic communications and data.[4] In this manner, custodians automatically condemn to purgatory the data of customers with the temerity to die without expressing their privacy preferences. Savvy trusts and estates practitioners routinely warn clients to assume that their fiduciaries will encounter resistance accessing online accounts and data, and to plan accordingly. Few online account custodians offer online tools that, as an alternative to passwords, would allow customers to control the access to and disposition of digital property held in such accounts, or even access to the records associated with the accounts. This flies in the face of longstanding public policy favoring the collection and preservation of a decedent's property.

The Uniform Law Commission (ULC)'s Revised 2015 Uniform Fiduciary Access to Digital Assets Act (hereafter, "Revised UFADAA") raised awareness of the problem, but provides only partial relief for those who fail to plan.[5]

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. 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). 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.

---

1 *See* https://coinmarketcap.com.

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

3 Jeff John Roberts and Nicolas Rapp, *Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says*, https://fortune.com/2017/11/25/lost-bitcoins/, accessed December 15, 2019

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

5 Unif. L. Comm'n., *Uniform Fiduciary Access to Digital Assets Act , Revised* (2015)..

Access to a decedent's emails might be important, perhaps for their sentimental value, but more likely because the decedent's email account contains the information necessary to continue a business or collect other assets. Technology companies, such as Apple, are increasingly emphasizing customer privacy and control over their data and accounts.[6] As a result, fiduciaries are not granted routine access to accounts, communications and other stored data, as they would have been automatically granted access to traditional assets in the past. A decedent or incapable person might have opened an online account with the expectation that the account would remain private and undiscoverable by anyone, including a fiduciary. Depending on the type of account, evidence of the account holder's intent may be required to show that the user intended the account to be accessible to others and not private.

This makes it vitally important to mention the importance of passcodes to clients with data stored on encrypted devices and online accounts. Fiduciaries who need to access a decedent's or incapable person's data and do not know the owner's passcode will likely be unable to obtain it without a court order.[7]

Terms-of-Service Agreements

Even if the fiduciary has a password, the account provider's terms-of-service agreement (TOSA) might forbid account access by anyone except the account holder[8]—implicitly barring a fiduciary from access. Online TOSAs are frequently silent about postmortem options and often simply prohibit postmortem access or transfer. Fiduciaries asking account providers for help accessing accounts are often completely rebuffed, or at best, forced to obtain court orders that authorize access and disclosure.[9]

Federal and State Anti-Hacking Laws

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.[10]

This criminalizes two kinds of computer trespass: accessing a computer "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 accessor is not entitled so to obtain or alter."[11]

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."[12] Because most internet servers are not located in the same state as a website's

---

6 Evan Niu, *Is Apple Hiding Behind Strong Privacy While Undermining Competition*?, https://www.nasdaq.com/articles/is-apple-hiding-behind-strong-privacy-while-undermining-competition-2019-11-28.

7 *See, e.g., Matter of Coleman* 2019 NY Slip Op 29067, 3/11/19, Surrogate's Court, Westchester County.

8 Yahoo!, *Yahoo Terms of Service*, http://info.yahoo.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 … ."

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

10 18 U.S.C. § 1030(a)(2)(C)(2012) (emphasis added).

11 *Id.* at § 1030(e)(6).

12 *Id.* at § 1030(e)(2).

users, internet use almost always involves obtaining information from a protected computer and therefore implicates the CFAA.[13] The term "computer" includes desktop computers, laptops, notepads, tablets, and smartphones.[14] Every U.S. state has an analogous statute, which varies in coverage, but typically prohibits unauthorized access to computers.[15]

Even when a fiduciary is expressly or impliedly 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.[16] 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 problem is that the account holder's digital accounts or assets are stored on the ***account 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.[17]

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

The Stored Communications Act

The Fourth Amendment to the U.S. Constitution generally prohibits the government from searching American 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 falls outside the coverage of the Fourth Amendment.[18] To fill that gap, in 1986 Congress enacted the Stored Communications Act (SCA) as a part of the Electronic Communications Privacy Act (ECPA)[19] 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.[20] The SCA regulates the relationship between the government, internet service providers ("ISP's"), and users in two distinct ways.

First, the SCA limits 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

---

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

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

15 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).

16 *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).

17 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., at 10

18 *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).

19 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. §§ 2701-2711.

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

or the content of any electronic communications in the absence of an applicable exception, such as consent by the account holder.[21]

The SCA permits, but does not require, ISP's to divulge non-content (or "metadata"), such as the user's name, address, connection records, IP address, and account information to a nongovernmental entity, such as a fiduciary.[22] Even the subject line of an email has been held to be content protected by the SCA, though.[23]

Second, the SCA limits the ISP's ability to voluntarily disclose communications content to the government or any other person or entity.[24] Generally, ISP's can only voluntarily disclose such content when the ISP's has the "lawful consent" of "the originator," an addressee or intended recipient of the communications, or the subscriber.[25] As a result, most ISP's 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.[26] While the highest court of one state has interpreted the SCA to allow ISP's to divulge the contents of a decedent's email account based solely on the executor's consent,[27] a federal decision will be necessary to ensure ISP compliance.

Perhaps the simplest way to provide fiduciary access to online accounts is by sharing the current account password. The practical problem with password sharing is the need to constantly update the list and address those inevitable provider-mandated resets. The legal problem is the risk of incurring civil fines under the SCA. One Massachusetts plaintiff won significant of 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 to his email account was unauthorized (i.e., she used the password for a reason her former partner had not authorized) under the SCA[28]. Despite very thin (or nonexistent) testimony to support the damage claim, the jury awarded the plaintiff $450,000 for the unauthorized intrusion.[29] Other juries have declined to make similar awards.[30]

I. Solutions

---

[21] 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).

[22] *Id.* at § 2702(c)(6).

[23] *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).

[24] *See* Kerr, *supra* n. 58, at 1212–1213 ("The statute creates a set of Fourth Amendment-like privacy protections").

[25] 18 U.S.C. § 2702(b)(3).

[26] 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. The court granted Facebook's motion to quash the subpoena but refused to address whether Facebook could voluntarily disclose the content. *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)).

[27] *Yahoo v Ajemian*, 84 N.E.3d 766 (Mass. 2017), cert. denied, No. 17-1005, 2018 WL 489291 (U.S. Mar. 26, 2018).

[28] See 18 U.S.C.A. Sec. 2701(a)(2).

[29] 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).

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

A. Password Managers. Account holders can avoid both issues by using a commercial password manager, since the password manager applications have the provider's permission to give access to the user's account.[31]

B. Online Tools. It's likely that the founders of most social media and other technology companies were worried about getting their platforms up and running and paying their rent, not their customers' death and incapacity. Had company founders had the luxury of contemplating incapacity and death when they created their products and services, 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.[32] 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 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). [33] Alternatively, the user can simply instruct Google to delete all account content.[34] 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. [35]

For those who fail to plan, Google's support policy 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.[36] 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.

Since 2015, Facebook's policy on postmortem account use and access has similarly provided for the designation of a "legacy contact."[37] The Legacy Contact feature currently provides that after an account is memorialized, the designated legacy contact can write a pinned post for the user's profile, view all posts, decide who can see and who can post tributes, if the memorialized account has an area for tributes, delete tribute posts, respond to new friend requests, update the user's profile picture and cover photo, request the removal of the account, turn off the requirement to review posts and tags before they appear in the tributes section, if the user had timeline review turned on, and download a copy of what the user had shared on Facebook, if this feature was activated.[38]

The legacy contact *cannot* read messages, remove friends or make new friend requests."[39] However, Facebook may allow an authorized representative (e.g., a family member) to obtain content

---

31 Popular password manager tools include LastPass, Dashlane, 1Password and KeePass, to name a few.

32 Google, *About Inactive Account Manager,* https://support.google.com/accounts/answer/3036546?hl=en (accessed December 15, 2019).

33 *Id.*

34 Id.

35 Id.

36 Google, Submit a Request Regarding a Deceased User's Account, https://support.google.com/accounts/troubleshooter/6357590?hl=en (accessed December 15, 2019)

37 Facebook Help Ctr., *What Is a Legacy Contact?* https://www.facebook.com/help/1568013990080948 (accessed December 15, 2019).

38 Facebook Help Ctr., *supra* n. 35.

39 Facebook Help Ctr., *supra* n. 35.

"in response to a valid will or other legal consent document expressing clear consent."[40] It may still allow an authorized representative to obtain content with a court order via a special request.[41]

Apple finally added its own online tool in 2021, which allows users to add one or more Legacy Contacts associated with each Apple ID. Those contacts can then ask Apple for access to the associated account data after the user's death, but they must have the access key generated when the user designated them as the contact, as well as the user's death certificate.[42] The Apple user can change the Legacy Contact at any time.

B. Revised UFADAA

To ensure that fiduciaries can access digital assets, ULC drafted the original Uniform Fiduciary Access to Digital Assets Act, or "UFADAA", which it approved in July 2014.[43] 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. [44]

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.[45]

Internet industry representatives also argued that the SCA requires the account holder's *express* consent to disclosure and that the account holder's presumed, or constructive, consent is insufficient. 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, and cited consumer demand for private, encrypted, anonymous services.[46] Privately, they expressed concern that offering postmortem access options during sign-up would scare away new customers.

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 months of increasingly difficult legislative battles, the ULC and technology industry representatives met and negotiated a compromise. The result was Revised UFADAA, which gives fiduciaries limited access to digital assets, while taking into account the privacy and contractual rights of account holders and compliance with federal and state privacy laws. It reorganized the original act and revised almost all of its provisions to make them less useful to fiduciaries and acceptable to account custodians. With the

---

40 Facebook Help Ctr., *What Data Can a Legacy Contact Download?* https://www.facebook.com/help/408044339354739 (accessed December 15, 2019).

41 Facebook Help Ctr., *How Do I Request Content From the Account of a Deceased Person? https://tinyurl.com/ookzqsl* (accessed December 15, 2019).

42 How to add a Legacy Contact for your Apple ID, https://tinyurl.com/2p8v9pyx (last accessed August 11, 2022).

43 Unif. L. Comm'n., *Uniform Fiduciary Access to Digital Assets Act* (2014).

44 Id..

45 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.

46 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).

resulting support of Facebook, Google and the endorsement of the American Civil Liberties Union and the Center for Democracy & Technology, to date, Revised UFADAA has been enacted in 44 US jurisdictions.[47]

A. Key Concepts

Revised UFADAA covers personal representatives, conservators, agents acting under powers of attorney, and trustees.[48] 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.[49] That third person can be a fiduciary or a "designated recipient" who need not be a fiduciary.

B. Disclosure

The original UFADAA provided most fiduciaries with default access to information protected by federal privacy laws. In contrast, Revised UFADAA requires a decedent's explicit consent for a personal representative to access the contents of a decedent's communications. When given, express consent overrides a TOSA's boilerplate prohibition against access or disclosure.

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).[50]

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. Levels of Access

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

---

47 Univ. L. Commn., *Legislative Fact Sheet —Fiduciary Access to Digital Assets Act,* Revised (2015), https://tinyurl.com/tt4gkyj (accessed December 15, 2019).

48 Unif. L. Comm'n., *Uniform Fiduciary Access to Digital Assets Act , Revised* (2015).

49 *Id.* at §§ 2(16), 4.

50 Id., at §4.

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.

2. Conservators. Conservator authority over assets in online accounts is quite limited under Revised UFADAA. 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. 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. 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 confirms that a trustee who is the original account holder will have full access to all digital assets. When a trustee is not the original account holder of the account, the trustee's authority is qualified, as Section 12 requires the settlor's consent for the disclosure of communications content. 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.

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, subsection (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. Thus, unlike the SCA, which merely permits disclosure, Revised UFADAA mandates it. 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.[51] 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. In exchange, Section 16(f) immunizes a custodian who complies with a request under the Act. In practice, custodians are uniformly insisting on court orders.

Section 3(b) 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.

II. 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 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).

III. 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.

[51] Based on notes of the Uniform Law Commission May 2015 meeting with industry representatives (on file with the author).