

By Suzanne Brown Walsh, Benjamin Orzeske & Turney P. Berry

You Can't Always Get What You Want

Understanding the revised Uniform Fiduciary Access to Digital Assets Act

Our clients want and need to control their digital lives and afterlives. They often have multiple online accounts with an equal number of passwords, some of which others know, some of which can be guessed and some of which are undiscoverable, at least by family members and advisors using legal means. Online and mobile banking have grown exponentially. Last year, a British Bankers' Association survey indicated that in the United Kingdom, bank customers made over £1 billion worth of transactions electronically every day, and they downloaded an average of 15,000 mobile banking applications each day in 2014, alone.¹ Few online account custodians offer customers online tools allowing users to provide for access to or disposition of any property held in such accounts, or even the records associated with the accounts, and only a few state probate codes provide defaults. Delaware enacted a comprehensive law in 2014.² Earlier state access laws, however, are much more limited.³

State and federal laws protect privacy and criminalize unauthorized access to computers and data. The terms-of-service agreements (TOSAs) and privacy policies that govern most digital accounts often create additional barriers to access.

Friends and families find it impossible to plan a wake, collect mementos, contact other friends and family members, sort through financial records or even pay

bills without access to cloud-based storage and email accounts. Most creditors and banks strongly encourage customers to "go green" and receive bills and statements electronically. Frequent flyer miles and other loyalty programs accumulate through online systems. Some clients conduct substantially all of their businesses and, in effect, earn their livings, online: bloggers, authors, artists or entrepreneurs. Indeed, some banks and financial institutions exist solely online with no brick and mortar stores or branches at all. Sometimes, digital dominance in a business means that even a traditional account is covered by the TOSA that was designed originally for a digital account.

Digital assets can have significant monetary value, including, of course, digital currencies, such as Bitcoin.⁴ There are currently about \$3.5 billion bitcoins in circulation.⁵ Perhaps the most unusual, valuable digital asset sold recently was a \$635,000 virtual space station in Entropia Universe, an online gaming platform.⁶

A fiduciary may find that certain assets or information belonging to an estate, which traditionally appeared in physical form—letters, tax returns, account statements, as well as music, art and literature—now exist only in digital form, as email, word-processed documents, spreadsheets, digital music, photographs, art or other unique digital content. This digital content may exist only on servers not controlled or owned by the decedent.

The revised Uniform Fiduciary Access to Digital Assets Act (revised UFADAA), which the Uniform Law Commission (ULC) approved on July 15, 2015,⁷ aims to ensure that a fiduciary has access to digital assets necessary and appropriate to enable the orderly administration of a decedent's estate.

Impediments to Fiduciary Access
Various policy concerns arise when thinking about fiduciary access to digital assets. Asking the question,

Suzanne Brown Walsh is a partner at Murtha Cullina in Hartford, Conn. **Benjamin Orzeske** (center) is chief of the Uniform Law Commission and is based in Chicago.



Turney P. Berry is a partner at Wyatt, Tarrant & Combs, LLP in Louisville, Ky.

“Did the creator of the asset want others to access it?” is too simple, although necessary. Most online accounts are password protected, and the data stored on a computer’s hard drive may be encrypted. Even if the fiduciary can find a password, the account provider’s TOSA might forbid account access by anyone except the account holder⁸—implicitly barring a fiduciary from access. Those contracts ought to mean something and be “overridden,” if at all, in a careful and limited fashion. While restrictive TOSAs won’t necessarily preclude fiduciary access, fiduciary access can’t be presumed. Further, digital communications, like traditional letters, raise privacy concerns for both sender and recipient.⁹ Do the senders and recipients of email view those communi-

The original UFADAA sought to place the fiduciary into the shoes of the account holder, resolving as many of the impediments to fiduciary access to digital assets as possible.

cations in the same manner as they might view a letter (recognizing that many of them may only have sent or received a few traditional letters)?

Federal and state laws also impede fiduciary access. At the federal level, the Computer Fraud and Abuse Act (CFAA) criminalizes the unauthorized access of computer hardware and devices and the data stored thereon.¹⁰ The U.S. Court of Appeals for the Seventh Circuit has clarified that the definition of “computer” includes home computers, laptops, notepads, tablets and smartphones.¹¹ Although few people read TOSAs, zealous federal prosecutors may use the federal CFAA to prosecute defendants based solely on violations of a website’s TOSA.¹² In addition, every state has an analogous statute that varies in coverage, but typically prohibits “unauthorized access” to computers.¹³

Congress enacted the Stored Communications Act (SCA) in 1986, as a part of the Electronic

Communications Privacy Act¹⁴ to respond to concerns over Internet user privacy. The SCA prohibits certain providers of public communications services from voluntarily disclosing the contents of electronic communications to the government or any other person or entity¹⁵ unless an exception to the SCA’s blanket prohibition against disclosure applies.¹⁶ The relevant exception for fiduciaries permits a provider to disclose communication contents if it has the “lawful consent” of “the originator” or an addressee or intended recipient of such communication[s], or the subscriber.¹⁷ Does that include the fiduciary who, under common law, “steps into the shoes” of the originator or recipient? That an act from 1986 imperfectly deals with technology matters 30 years later isn’t surprising.

Original UFADAA

To make certain that fiduciaries have the access to digital assets they need, the ULC drafted and approved the original UFADAA on July 16, 2014.¹⁸ It was based in asset neutrality: Fiduciaries ought be able to access digital assets as easily as assets stored on paper.

The original UFADAA sought to place the fiduciary into the shoes of the account holder, resolving as many of the impediments to fiduciary access to digital assets as possible. It gave the fiduciary “the lawful consent” of the originator/subscriber so that the provider could voluntarily disclose the files pursuant to the second relevant provision of the SCA.¹⁹

Many in the Internet industry also believe that the SCA requires the account holder’s express consent to disclosure and that the account holder’s constructive consent is insufficient.²⁰ But, the original UFADAA was premised on the notion that the fiduciary had the account holder’s implied consent and didn’t need actual consent. This disconnect presented difficulties as state legislatures began considering the original UFADAA.

Internet providers in many instances also objected to the original UFADAA’s override of their TOSAs. If a TOSA made certain promises to a customer that the provider couldn’t fulfill because of the original UFADAA, what obligations did that impose on the provider? They were also concerned that presenting their account holders with post-mortem access options during sign-up would scare away new customers by making the enrollment process more difficult and time consuming, and all of those issues would create

administrative burdens that are unquantifiable.

Many privacy advocates worried about the original UFADAA as well, focusing on the core question of whether email is different in some fundamental way from earlier forms of communication.²¹ Some argued it was, by virtue of the automatic archiving feature that most email services provide. Finally, some providers noted the consumer demand for private, encrypted, anonymous services and wanted to ensure that those wouldn't be affected.

Revised UFADAA

After a year of legislative battles, the ULC and technology industry representatives met and negotiated a compromise—the revised UFADAA, which reorganized the original UFADAA and revised almost all of its provisions.²² While it retains the original UFADAA's comprehensive scope and applies to personal representatives, conservators, agents under powers of attorney and trustees, the revised UFADAA also contains some of the provisions of the restrictive industry bill known as the Privacy Expectations and Afterlife Choices Act.²³ As a result, Facebook supports the revised UFADAA, as does the Center for Democracy and Technology.²⁴

Key concepts and definitions. An “online tool” is an electronic service that allows a user, in an agreement that's distinct from the TOSA, to provide directions for the disclosure or non-disclosure of digital assets to a third person. That third person given access to the digital assets can be a fiduciary or a “designated recipient,” who needn't be a fiduciary. A “digital asset” is an electronic record in which an individual has a right or interest, not including an underlying asset or liability unless the asset or liability is itself a record that's electronic. This asset includes both the catalogue, or log, of electronic communications and the content of electronic communications, but it would exclude securities or traditional currency. For example, neither securities held in street name nor money in a bank are digital assets. The revised UFADAA simply addresses the fiduciary's right to access all relevant electronic communications and the online account that provides evidence of ownership.

Fiduciaries' access limited. The original UFADAA provided most fiduciaries with default authority over and access to information protected by federal privacy law. In Section 4, the revised UFADAA instead provides that users may consent to disclosure of protected elec-

tronic communications content either in an online tool or in a record (that is, in a will, power of attorney or trust instrument). Such express consent will override a TOSA's boilerplate prohibition against access or disclosure. Without express consent, the revised UFADAA doesn't require custodians to disclose user content, but does require disclosure of digital assets other than private electronic communications.

In short, the revised UFADAA won't help a fiduciary for any individual who hasn't engaged in at least the most basic estate planning recover that individual's electronic communications. Federal law and a respect for the contracts—the TOSAs—signed by individuals,

Happily, for those who do allow fiduciary access in estate-planning documents, the revised UFADAA is an enormous help.

appear to mandate this result in the current environment. Happily, for those who do allow fiduciary access in estate-planning documents, the revised UFADAA is an enormous help.

The revised UFADAA Section 5 expressly preserves the custodian's TOSA provisions, except as is necessary to effectuate a user's express consent to the disclosure under Section 4.

The revised UFADAA Section 6 allows the custodian to determine whether to grant the fiduciary full access to an account, 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. The disclosures don't include deleted assets, and the custodian may charge a reasonable fee. It also contains provisions protecting custodians from unduly burdensome requests.

Personal representatives. The revised UFADAA Section 7 gives the personal representative limited access to 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 consent to disclosure. 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 at the custodian's option.²⁵ 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.²⁶ Thus, Section 8 was intended to give personal representatives default access to the "catalogue" of electronic communications and other digital assets not protected by federal privacy law.

Conservators (including guardians). The revised UFADAA Section 14 permits a court to authorize conservator access to digital assets after the opportunity for a hearing. It doesn't permit conservators to request that a custodian disclose a protected person's electronic communications 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.

Agents acting under powers of attorney. The revised UFADAA Section 9 provides that an agent has authority over a principal's electronic communications content only if the principal expressly grants that authority, just as in the original UFADAA. Thus, access to content of electronic communications by an agent is a "hot" power (meaning that 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.

Trustees. The revised UFADAA 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's the original account holder will have full access to all digital assets. For assets that the settlor transfers, a trustee isn't the original account holder of the digital assets, and the trustee's authority is qualified and is governed by Sections 12 and 13. Thus, Section 12, governing disclosure of content, requires consent, and Section 13, governing all other digital assets, doesn't.

Access and transfer of the digital assets into the trust would be accomplished by the settlor (while alive and capable), the settlor's agent or a personal representative.

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

Fiduciary duty and authority. The revised UFADAA Section 15 specifies the nature, extent and limitation of the fiduciary's authority over digital assets. Much of this section simply restates existing state law but because many readers of the revised UFADAA aren't in the trust and estates field, the restatement was thought helpful. Thus, Subsection (a) expressly imposes fiduciary duties such as care, loyalty and confidentiality, and Subsection (b) subjects a fiduciary's authority over digital assets to the TOSA, except to the extent the TOSA provision is overridden by an action taken pursuant to Section 4, and it reinforces the applicability of copyright law and fiduciary duties. Subsection (b) also prohibits a fiduciary from impersonating a user. Subsection (c) permits the fiduciary to access all digital assets not in an account or subject to a TOSA but Subsection (d) further specifies that the fiduciary is an authorized user under any applicable law on unauthorized computer access. Finally, Subsection (e) clarifies that the fiduciary is authorized to access digital assets stored on devices, such as computers or smartphones, without violating state or federal laws on unauthorized computer access.

Importantly, Subsection 15(f) gives the fiduciary the option of requesting that an account be terminated, if termination wouldn't violate a fiduciary duty. Closing accounts in a timely manner is key to minimizing the risk of fraud and abuse and, in some instances, is a significant element in creating a care plan for an individual.

Custodian compliance and immunity. If a fiduciary has access under the revised UFADAA and properly substantiates his authority, a custodian must comply with the fiduciary's request for disclosure or termination within 60 days of its receipt of all of the required documentation. If the custodian doesn't comply, the fiduciary may apply for a court order directing compliance, which must contain requisite findings of fact.

The revised UFADAA Subsection 16(c) gives custodians the right to notify a user that the fiduciary has requested disclosure or termination, and