A little over 10 years ago, the first iPhone was introduced to the world, thereby kickstarting a relationship and dependence on technology that transformed conventional views on digital property and digital assets. As consumers began using and integrating their smartphones into everyday life, estate planners soon realized that comprehensive estate planning must include digital planning and the safeguarding of clients' digital assets, footprints and online identities. From an estate administration perspective, fiduciaries faced new challenges in identifying and marshalling digital assets because probate laws did not contemplate such rapid developments in digital property, and legislators were unable to keep pace with technological advancements. Now, a decade later, executor access to digital assets and data is still restricted by antiquated 20th century laws.

Before diving into the “how” of administering estates with digital assets, we first must understand both the term “digital assets” and the current state of the law with respect to an executor’s ability to access a decedent’s digital assets and digital data. The term “digital assets” includes cryptocurrencies, digital documents, photographs, music and electronic banking information, just to name a few. Do you have an email account? What about a Facebook, Instagram, LinkedIn or Twitter account? Do you store files using a cloud-based storage service or even just an electronic folder on a personal computer? These are all digital assets, and an executor’s rights to these assets are typically governed by the individual Terms of Service Agreement (TOSA) that the deceased user “agreed” to with respect to each asset or piece of data.

Clients rarely consider the prevalence of digital property in their lives, the number of TOSAs that apply to their specific digital assets or the ability (or lack thereof) of their executors to access digital files. Thus, digital assets may be some of the most important, but least planned for, assets in a decedent’s estate. Take this article, for example. Initially, the authors dictated the article into a Microsoft Word app on an iPhone with the help of Siri (thereby applying the TOSAs of Microsoft and Apple). A draft was then stored on each of their Dropbox accounts (applying Dropbox’s TOSA). The drafts were then emailed back and forth using their Yahoo and Comcast email accounts (applying Yahoo’s and Comcast’s TOSA), the two drafts were combined into a single document in Microsoft Word (again triggering Microsoft’s TOSA), and a final draft was uploaded to Google Docs to enable the authors to jointly collaborate on the article (applying Google’s TOSA). What if one or both of the authors had died in the process of writing the article – how would their executors access the article? Which TOSAs would apply and to what version of the article? What if, instead of an article (which we acknowledge has little monetary value), we were collaborating over a priceless manuscript or a musical score or groundbreaking medical research? As digital assets and digital data become more prevalent and more common, executors must have the ability to access a decedent’s digital assets during the administration of a decedent’s estate, just as they have the ability to access a decedent’s “traditional” assets.

Continued on page 7
Administering Estates with Digital Assets
Continued from page 6

Federal Law

In 1986, Congress passed the Stored Communications Act (SCA) in an effort to protect a user’s private digital information from unauthorized disclosure. The SCA provides that a user or entity providing electronic communication service shall not knowingly divulge the contents of a communication electronically stored by the service provider. Such an unauthorized disclosure will subject the offender to criminal liability. An exception to the SCA exists, however, if the originator or intended recipient of such communication provides “lawful consent” to the disclosure of such private digital information. The SCA is silent as to its applicability to fiduciaries and whether a decedent may lawfully consent to the disclosure of such information to such decedent’s executor. As a result, in order to protect themselves from potential criminal liability, service providers and custodians of digital assets have been hesitant (and in some cases even refused) to disclose a decedent’s electronically stored information to executors.

Also in 1986, Congress passed the Computer Fraud and Abuse Act (CFAA) in an effort to combat the hacking of electronic devices and the unauthorized access of digital information. The CFAA criminalized the unauthorized and intentional access of computers and devices. As with the SCA, the CFAA is silent as to its applicability to fiduciaries and whether executors possess the requisite authority to access a decedent’s digital assets. The CFAA therefore affords executors no protection to access a decedent’s digital assets and exposes an executor to potential criminal prosecu-

The CFAA therefore affords executors no protection to access a decedent’s digital assets and exposes an executor to potential criminal prosecu-

tion if the executor unlawfully accesses the decedent’s digital information.

State Law

Following Congress’s lead, all 50 states, including Pennsylvania, passed their own versions of the CFAA. Pennsylvania’s version criminalizes unauthorized access to any computer, computer system, computer network or internet site with the intent to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises. For example, if an executor logged into a decedent’s email account using the decedent’s login information and password, such an action could be construed as a violation of Pennsylvania law because the executor intended to access the decedent’s information, did not have authorization to access the information, and obtained access through false pretenses or misrepresentations (i.e., impersonating the decedent through the use of the decedent’s username and password). Pennsylvania’s law therefore severely restricts an executor’s ability to legally access a decedent’s digital assets and digital data.

Uniform Fiduciary Access to Digital Assets Act

In an effort to unify and clarify state laws with respect to an executor’s ability to access a decedent’s digital assets and digital information, the Uniform Law Commission introduced the Uniform Fiduciary Access to Digital Assets Act (UFADAA) in July 2014. UFADAA was designed to allow a fiduciary to stand in the shoes of the decedent such that the decedent was presumed to have lawfully consented to the decedent’s executor’s access to the decedent’s digital assets and digital data. UFADAA was not designed to expand an executor’s access or authority over a decedent’s digital assets and digital data beyond that originally possessed by the decedent. UFADAA was simply drafted to fall within the lawful consent exception to the SCA and to provide executors with a safe harbor from the CFAA and corresponding state statutes so that executors could possess the ability to access and control a decedent’s digital assets and digital data without fear of criminal prosecution.

UFADAA, however, faced significant opposition from custodians of digital assets and digital data. First, critics attacked UFADAA on the grounds that decedents wanted to preserve their digital privacy and had no intention of automatically granting their executors authority to access their private digital assets. Next, custodians argued that UFADAA was preempted by the SCA and CFAA, which did not provide for an “executor’s exception.” Finally, custodians claimed that UFADAA would invalidate and nullify their existing TOSAs.

Revised Uniform Fiduciary Access to Digital Assets Act

In September 2015, the Uniform Law Commission introduced the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). Unlike UFADAA, which presumed a decedent’s consent for the decedent’s executor to access his or her digital assets, RUFADAA places the burden of consent on the decedent to specifically provide lawful consent in the decedent’s will for the executor to access and manage the decedent’s digital assets. In the absence of a provision in the decedent’s will providing lawful consent, each TOSA will govern the decedent’s respective digital assets and an executor’s ability to access and manage such digital assets.

RUFADAA also provides for the

Continued on page 8
Administering Estates with Digital Assets

Continued from page 7

ability of a user to use an “online tool,” which is an account-specific feature the custodian may offer to its users to enable a user to direct the custodian to disclose (or not disclose) digital information to a designated recipient, including the content of an electronic communication. Such an online tool would override both the terms of a TOSA and the decedent’s will.

RUFADAA provides that a custodian has the sole discretion to grant an executor full, partial or no access to the decedent’s account or provide the executor a copy of the digital asset. If a deceased user consents or if a court so directs, a custodian shall disclose the content of an electronic communication to the executor. Regardless of the deceased user’s consent, an executor may request a catalogue (but not the content) of a decedent’s electronic communications.

Administering Estates with Digital Assets

Pennsylvania has yet to pass any form of either UFADAA or RUFADAA, thereby forcing executors to address the access and control of a decedent’s digital assets based upon federal laws created in the 1980s. At some point in the future, Pennsylvania will pass some form of legislation to address fiduciary access to digital assets. In the meantime, digital assets of decedents in Pennsylvania must still be marshalled and dealt with accordingly. Below are a series of steps that any executor should consider when administering an estate with digital assets, depending upon whether the executor is administering the estate with or without a RUFADAA-type statute.

Step 1: Obtain Custody of Digital Assets

Under RUFADAA, the executor must first look to the decedent’s will to determine whether the decedent provided lawful consent to the executor to access and manage the decedent’s digital assets. Assuming that the will provides such lawful consent, the executor should contact the custodian of the digital asset and provide the custodian with a copy of the decedent’s will and a copy of the executor’s appointment papers that authorize the executor to act on behalf of the decedent’s estate. The executor should then be able to access both a catalogue and the content of the decedent’s digital asset. If the decedent’s will is silent as to lawful consent, then the executor should carefully review the TOSA to determine how the custodian will treat the decedent’s digital asset upon the decedent’s death. The executor should also contact the custodian and seek a catalogue of the decedent’s digital asset.

In non-RUFADAA jurisdictions, it is unclear as to whether a decedent may lawfully consent in his or her will to the executor’s access and management of the decedent’s digital assets. In the absence of RUFADAA-type statutes, it is likely that a decedent may not provide such lawful consent, thereby causing the executor to rely exclusively on the terms of the TOSA to govern the executor’s ability to access and manage the decedent’s digital assets. Unless the TOSA so provides, the executor will have no right to a catalogue or the content of the decedent’s digital assets.

If the executor has lawfully obtained access to the decedent’s digital assets, the executor should begin the process of gathering the decedent’s digital assets and searching for additional digital assets. If the executor is only able to access a catalogue of the decedent’s digital assets, the executor should carefully review the catalogue in the hopes of locating the decedent’s other digital assets.

Step 2: Inventory and Consolidate Digital Assets

Assuming that the executor has gained lawful access and control over the decedent’s digital assets in either a RUFADAA jurisdiction or a non-RUFADAA jurisdiction, the executor should inventory all of the decedent’s digital assets and then consolidate the digital assets in the decedent’s estate. For example, the executor could forward all of the decedent’s email accounts to a single account, the executor could consolidate cryptocurrencies, and the executor could store photos, music and videos in a single location.

The executor should determine if any automatic payments are being made from the decedent’s accounts and whether to stop such automatic payments. The executor will likely want to pay the decedent’s debts and the estate’s administration expenses out of an estate account in order to better account for the transactions of the executor. The executor may also want to keep certain accounts open for an extended period of time to determine whether any other assets or creditors exist.

Step 3: Safeguard the Decedent’s Digital Assets and Digital Identity

Once the executor gains access and control over the decedent’s digital assets, the executor must also safeguard the decedent’s digital assets. The executor should restrict other users from accessing the decedent’s digital assets, store the digital assets in a secure location that is only accessible to the executor and change the decedent’s passwords. If lawfully permitted to do so, the executor may even want to

Continued on page 12
back up the digital assets by creating copies of the digital assets and archive the digital assets so that they may be maintained and accessible during any relevant statute of limitations period.

The executor should take steps to safeguard the decedent’s digital identity. This would include contacting custodians to remove the decedent’s personal data from websites, removing the decedent's social media accounts and searching the internet for any evidence of a decedent’s continued online presence. The executor may want to email the decedent's contacts to place them on notice that the decedent has passed and to be on the lookout for any unauthorized use of the decedent’s digital assets or digital identity.

Step 4: Valuing Digital Assets

Just as non-digital assets must be valued, digital assets must be valued for estate and inheritance tax purposes or for distribution purposes. Some digital assets, such as cryptocurrencies, may be easily valued, while other digital assets may be more difficult to value. Some digital assets may have sentimental value but little monetary value. Ultimately, difficult-to-value digital assets may require the use of specialized valuation experts to ascertain the fair market value of the asset on the date of the decedent’s death.

Step 5: Disposal/Distribution of Digital Assets

When the executor is ready to close the decedent’s estate and distribute the remaining assets to the beneficiaries, the executor should either distribute the decedent’s digital assets or delete the decedent’s digital assets in a manner that will safeguard the decedent’s identity. The executor should pay special attention to the terms of the decedent’s will and the TOSA, as the TOSA may contain restrictions on the transferability or deletion of the decedent’s digital assets.

Ultimately, executors face many hurdles in administering estates with digital assets. Until Pennsylvania adopts a version of RUFADAA to provide clarity for executors to access a decedent’s digital assets, executors will continue to struggle with the ability to marshal, access and control a decedent’s digital assets. Even after a version of RUFADAA is adopted, executors will continue to face new challenges in administering estates with digital assets.

Justin H. Brown is a shareholder at Flaster Greenberg PC, where he focuses his practice on estate, tax and asset protection planning, estate administration and estate litigation.

Ross Bruch is a wealth planner at Brown Brothers Harriman & Co. and focuses on values-based wealth planning for ultra-high net worth families and closely held business owners. Ross also serves as the chair of the Technology Committee for the Philadelphia Bar’s Probate and Trust Law Section.