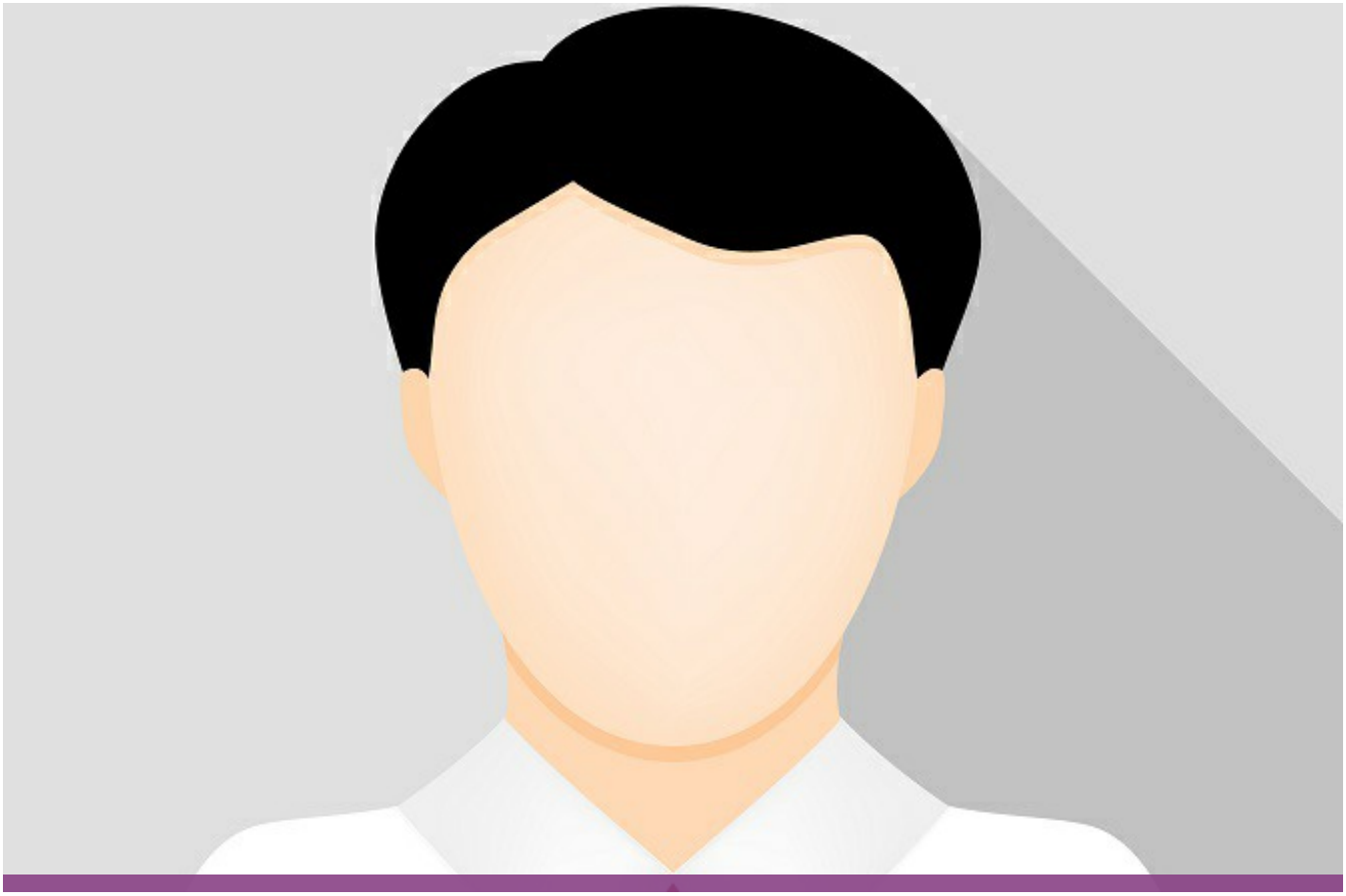
Digital life after death



| Wednesday, April 6, 2016

For anyone who has dealt with the death or incapacity of a loved one in recent years, one of the most perplexing and fraught questions has been how to access their electronic or digital records. Whether we realize it or not, most of us own digital assets. These could be photographs or videos on your smartphone, documents in the cloud, iTunes music collections, email accounts, social media accounts, banking records, online shopping or travel memberships, stock trading accounts – anything that can be created, transmitted, accessed or stored on any electronic or digital medium.

As central to our lives digital assets have become, very few of us make specific arrangements for handling access to and disposal of our digital assets in the event of our death or incapacity. Collecting digital assets and closing down online accounts after death or incapacity are important for various reasons, including the prevention of fraud, identity theft and other cybercrimes. Even though we may think that leaving a record of our passwords and security questions for our loved ones is enough to allow them to take care of our digital life, few of us realize that this is inadequate. In reality, the terms-of-service agreement and privacy policy each of us breezes by on our way to setting up our online accounts give the online provider, or custodian, of the information dictatorial power over mom's or dad's email accounts and the like. Many such agreements provide that no one other than the registered user of the account may access it.

Moreover, federal laws, such as the Stored Communications Act (and its larger vehicle, the Electronic Communications Privacy Act) and the Computer Fraud and Abuse Act, generally prohibit and criminally penalize unauthorized access to computers and to certain forms of protected data, such as email communications. Laws in many states, including Florida, also provide similar protections. Generally, questions of authority, agency and inheritance are questions of state law unless the federal government has preempted the field. The question under any of these laws is "what constitutes authorization?" Aside from specific laws such as the Gramm-

Leach-Bliley Privacy Act and HIPAA, there is no federal or uniformly applicable law addressing the question of third party access to digital assets as digital assets on a broad scale. Just because someone provides another with a username and password, it does not completely protect the recipient from potential violations of federal law.

Effective July 1, 2016, Florida will join a dozen states that have enacted legislation regarding access to the digital assets of the deceased or incapacitated. It is only one of five states to have adopted the Uniform Fiduciary Access to Digital Assets Act (UFADAA or the Act). The Act is substantially based on the most recent model law drafted by the Uniform Law Commission regarding fiduciary access to digital assets. Over two dozen states, including Illinois and Michigan, currently have similar bills before their legislatures. But a coalition of industry players and privacy advocates has voiced opposition and gone on record with respect to perceived problems with the implementation of digital asset access bills, holding up or defeating passage in a number of states. Among these are concerns about third-party privacy, conflict with federal law and proper authentication of authorizing documents to prevent fraud.

Florida's 2016 legislation avoided the fierce opposition that killed a similar bill in 2015 after the Senate sponsor, Senator Dorothy Hukill, reworked it to clarify that the user's express consent is required before anyone can take over the user's digital assets. It then passed without a negative vote on the floor. Governor Rick Scott signed it into law on March 10, 2016. As the state with the largest population of persons over the age of 65 in America, Florida has a significant interest in addressing the digital needs of its aging population and their survivors. Florida's law applies only to the digital assets of persons who reside in the state or who resided in the state at the time of death.

Users can designate via online tool or by separate writing

The Act defines a "digital asset" as an electronic record in which an individual has a right or interest. Its fundamental premise is that the user, that is, the owner of the digital assets in question, has absolute control to designate whether or not he wants his personal representative, trustee or agent (i.e., attorney in fact) to have access to some or all of his digital assets in the first place. In the absence of express consent by the user, the terms-of-service agreement controls. Consent under UFADAA is evidenced in one of several ways. An "online tool" provided by the online provider or custodian of the digital assets is the paramount basis for authority.

Currently, few, if any, custodians offer an online tool. Facebook™ created a "Legacy Contact" option last year, which allows the account owner to appoint someone to accept friend requests, change the profile picture and pin a post on the timeline, but does not allow access to Facebook messages or permit direct posts in the departed user's name. The user also can direct Facebook to terminate the account.

Instead of choosing the online tool, the user may specifically provide in a will, trust agreement or power of attorney that a designated fiduciary appointed under one of these instruments may access the digital accounts. A settlor who also serves as her own trustee, such as in a revocable trust, is presumed to have unbridled access to her own digital assets, including electronic communications, if they have been placed in the trust. The user also can create a designation in a separate digital assets will, trust or power of attorney, provided it complies with the same formalities for execution as any similar instrument under Florida law. Even if these were executed or the user died prior to the effective date of the law, July 1, 2016, their designations are valid under UFADAA.

If there's a conflict between the designation made via the online tool and a designation in the will, trust, or power of attorney, the designation in the online tool controls if the online tool permits the user to modify the designation at any time. So, if you select "termination" for your Facebook account in the Legacy online tool, it dies with you, and no one can revive it.

Florida's UFADAA also provides that nothing in the law grants the fiduciary or designated recipient any greater rights than those provided the user in the terms-of-service agreement. The designation also can be overridden later by the user herself, by federal law, or even by a terms-of-service agreement if the user did not use an online tool to make the designation.

Notably, UFADAA limits acceptable designees according to how they are appointed. The user can appoint a friend or family member, as well as a fiduciary, using the online tool. Otherwise, a friend or family member cannot obtain access to digital assets of the user unless he or she is also the appointed fiduciary. A fiduciary can be either a natural person or a professional institutional fiduciary.

Electronic communications still private unless user specifically grants access

The user may declare that she wants her designee to have complete access to all digital assets, including electronic communications, or may restrict access to only certain types of assets. For example, she can permit her personal representative to access her photo albums or literary papers stored in the cloud, but not her emails or text messages. Unless she specifically states that she wants to grant access to the contents of electronic communications, the custodian may not release such content to the fiduciary. Such authority may be contained in a will, trust, power of attorney or "other record evidencing the user's consent to disclose the content of electronic communications." But aside from defining what a "record" is, UFADAA does not establish what kind of formalities that record must meet or how the record itself must be authenticated.

There's a catch, however. Unless the user specifically prohibited disclosure of digital assets or a court order so provides, the fiduciary can require the custodian to provide a catalog of the digital assets, including the name of each person, account and email address with whom the user exchanged electronic communications, and the date of such communications. Neither the subject line nor content may be released. But the custodian can require the fiduciary to provide an affidavit stating that disclosure of the user's digital assets is necessary for administration of the estate, or a court order so finding, as well as certain specific information about the account. Although the Act does not describe what might fulfill this necessity requirement, reasons that come to mind include distributing digital assets in accordance with a will; accessing tax and financial information, legal documents, business papers, agreements, property inventories; preserving digital copies of artwork or draft manuscripts; establishing competence at a certain point in time; or, locating evidence.

It's not difficult to imagine how this particular provision can create angst. Granting access to digital assets is like giving others the key to your diary. Lots of secrets will be spilled. What if the decedent was having an extra-marital affair and exchanging constant text messages with his or her lover? If the surviving spouse also is the designated fiduciary, some less than pleasant scenarios can arise. Does the other party to the text have a privacy right not to have others know that he or she was on the other end of a torrent of text messages with the deceased at 3 a.m. every night? Or, in a less scandalous scenario, where multiple family members are involved, will the child fiduciary of the decedent have her feelings hurt to know that her mother was constantly emailing with her estranged younger brother? In the context of family and human relationships, anything is possible. UFADAA does not deal with these scenarios and creates no procedure by which third parties can participate in challenging access.

Friends and Family vs. Fiduciary Designations

In light of the possibility that digital asset planning can result in unintended controversies, before making a designation, the owner of the digital assets should think carefully about what access rights to give someone and who that person should be. When a user grants less than complete access, the custodian has the option to refuse to sort through the user's information if it presents an undue burden. The custodian also can limit the disclosures by date or ask the court for direction. In any case, a custodian may charge the fiduciary the reasonable cost of complying with the user's designations. Although a fiduciary is already bound to certain standards (such as the duty of care; the duty of loyalty; the duty of confidentiality), to avoid any doubt, it would be prudent to specifically stipulate in the digital access instrument that the fiduciary may not disclose the contents of emails and text messages or information about third party senders or recipients to anyone else. Designating one's lawyer either in the online tool or fiduciary appointment probably is a prudent choice under most circumstances, since attorneys are already under an ethical obligation to preserve client confidentiality. But it may not be the most practical or economical option.

Custodian safeguards and immunity

UFADAA provides many safeguards to ensure that the custodian is granting access only to an authorized designee of the actual account user. Among other things, the fiduciary must provide a certified copy of the appointing instrument (assuming the user did not use the online tool) or a court order containing certain findings as to the fiduciary's authority. In the case of a deceased user, the personal representative must have obtained letters of administration or other similar order from the court. Adequate proof that the user owned the account in question is also required. And the custodian may request additional information. The custodian also has the option of seeking a court order in the event of any doubts. Once all the requested information has been provided to the custodian, it has 60 days within which to grant access to the designee to the extent authorized in the user's designation. Nothing in the Act requires the custodian to restore deleted information. But the custodian has complete discretion in how it grants such access. It can let him access the account like a normal user, or it can extract the information in digital or paper form.

As long as the custodian acts in good faith in complying with UFADAA, it has no civil liability. However, as a state law, UFADAA cannot exonerate a custodian from violation of federal law. A custodian may not, for example, grant access to music collections and the like if such access violates copyright law. Therefore, custodians will want to confirm that federal law does not prohibit compliance with a specific UFADAA request. In Florida's version, the user, a subsequent federal law or modified terms-of-service agreement can terminate or modify the designee's access under the Act if the user has not provided direction using the online tool. The designee can seek an order in state court to enforce UFADAA against a custodian.

Digital assets outside UFADAA

UFADAA does not affect what the fiduciary can do with any information stored in the actual devices that may fall within a bequest or grant of "all personal property" of the user in a will or trust. A fiduciary who has been granted control of someone's computer, external drive, or cell phone can explore those at will, just like she could do in going through someone's personal papers and effects.

Nor does UFADAA apply to a digital asset of an employer used by an employee "in the ordinary course of the employer's business." In light of this, a business owner whose company has its own enterprise server that the owner uses for his personal matters should take the extra step of having the company's privacy policy provide for turning over certain digital assets to an appointed fiduciary under UFADAA. Further, all employers should review their employee handbooks, privacy policies and terms-of-use to anticipate potential requests by employees' designees and avoid potential disputes as to whether personal emails or records on the company's systems, mobile phone accounts or issued devices belonged to the employee or belonged to the employer and were "in the ordinary course of the employer's business."

Involuntary guardianship and digital assets

So, what happens when someone becomes incapacitated without having previously designated an authorized recipient? If the user is placed in involuntary guardianship, UFADAA also applies, even if the guardian was appointed prior to the Act's effective date. In the case of sudden incapacity, absent prior selection by online tool, the user has not intentionally granted anyone permission to access his digital assets. In such case, a court-appointed guardian must obtain a court order after a duly noticed hearing to establish a right of access to digital assets. However, unless the court or the user directs, the custodian may not provide access to any electronic communications to the guardian. It may, however, provide a catalog of the communications. If the guardian has general power over the user's affairs, for good cause he can request the custodian to suspend or terminate the ward's account. Nothing in the Act defines "good cause," but if the custodian charges fees for the account, preserving the ward's assets should satisfy this requirement. Other possible "good cause" should include a showing that the ward could be subjected to fraud or identity theft through a dormant account or is incapable of making proper decisions for his or her welfare and is in physical or financial risk by retaining unfettered access to online accounts.

Planning is essential

As with our family, financial assets and health care directives, planning ahead for our digital assets is important. It can save our loved ones significant stress and make it easier for our trusted fiduciaries to carry out their obligations. It can protect our other assets and prevent criminals from stealing our identities. On the emotional side, a treasure trove of photographs or music downloads in digital form may be every bit as valuable and cherished as the old family photo albums and vinyl collections. Thoughtful designations in advance can also carry out our desires with respect to whether we want our "digital selves" to live on long after we have departed this life.