When You Die, Will Your Digital Assets Go to Hell?

By Sharon D. Nelson, Esq. and John W. Simek

Introduction

Facebook only arrived on the scene in 2004. It seems to many, especially the young, as though it has been here forever, but it has not. Our children simply don't remember a non-digital life. So much has changed in the last two decades that we find ourselves trekking on unmarked paths in a new frontier. We now – and forevermore – will live in a digital world. Those who are disconnected have become dinosaurs, dying out slowly over time. Change is forced upon us.

Most people have no understanding of the digital property they own, and even less understanding of what may happen to those assets if they die or become incapacitated.

The Definition of Digital Assets

Wouldn't it be nice if we had a standard definition? Dream on. Even if we did, technology would continue to morph and our definition would be outdated.

We can't even seem to agree on whether to call it "digital assets" or "digital property" – for the moment, the terms seem to be used interchangeably.

Digital property is everywhere and what it constitutes is broad – e-mail, texts, social media posts, blogs, online accounts (including real life value of some assets in virtual worlds such as Second Life), videos, passwords and IDs to access sites, data you may have on shopping, financial and other sites, electronic documents (think of your old tax returns as an example), online backups, photo collections, airline miles, hotel rewards, books, movie scripts, etc. To the dismay of many, it does not include your iTunes music collection, e-book reader books or movies you downloaded because you purchase only a license – you don't own the music, books or movies. The licenses typically expire when you die – and sometimes much sooner.

If you think “pish, posh, what can these things be worth?” bear in mind that 10 domain names have sold for $7-$35 million in the last 11 years. And that is only one kind of digital property! Consider how many millions are now held as digital currency in Bitcoin wallets. Good luck in discovering those if someone is trying to hide them.

It is beyond the scope of this article to tell you how each site or online provider will handle your data in the event of your death or incapacity. You actually have to read the Terms of Service (ToS) for each site to see whether an executor may have access to the data, may memorialize your site, may remove it, or whether your site will terminate automatically after a given period of inactivity, etc. Even where an executor may be allowed some power with relation to digital property, a court order may be required under the ToS which can make managing the assets a costly and lengthy process.

Recently, online providers have begun developing online tools to allow you to express your wishes (think of it as a digital will) – and they generally take priority over the ToS. Google’s Inactive Account Manager is a good example. By completing the required form, you have control over what happens to your account. Facebook will memorialize your account but immediate family can request removal of the site. The user can also define a Legacy Contact to manage a memorialized site and authorize the Contact to download what you’ve shared on Facebook.

Microsoft has a Next of Kin process for e-mail accounts – if you provide an official death certificate, or proof of incapacitation, and proof that you are the next of kin or executor, you can delete and close accounts or have their contents shipped to you on DVD. Twitter will delete an account only after receiving proof of a user’s death. Basically, an online search for “What happens to my (insert name) account when I die?” will give you links to online help.

Estate Planning and the Challenges of Digital Assets

Estate lawyers have only begun to think about planning for the disposition of a client’s personal and business digital property in the last few years. We still lecture to lawyer audiences who remain fundamentally clueless about how to handle digital assets.

Digital property is often hidden from view. A client's loved ones may have no idea what property exists or where to find it. The best advice we can give clients is to keep a detailed list of their digital property with access information - user name, password, PIN, security question and answer, and who has access or at least how to access an "asset vault" of all of the required login data. This digital inventory will be useful to clients who can then prepare a digital property memorandum for their estate attorneys.

Leonard Bernstein, the famous composer, died with his autobiography ("Blue Ink"), in a password-protected file so secure that more than a decade later it still has not been accessed.

Many of us opt out of paper financial statements but without them, executors may not know of assets – or we may not know of bills that need to be paid. We recommend keeping data in an encrypted electronic file for security and identity theft reasons, but making sure that someone you trust has the credentials necessary to get to that document, which must be continually updated. A password protected Word document or Excel spreadsheet is a fairly simple and common solution. A password will encrypt the contents, but make sure you use a strong password.

We continue to hear stories of a husband or wife who handles all the paying all the bills but doesn't share the online banking credentials with their spouse. Depending on the laws of your state, they may not be given access to the online account and may need a court order to get access to the actual bank account. We've seen an instance in Virginia where the wife, who was the Executor, had to close the account and open a new one just to get control of the new account online. In the meantime, bills went unpaid and interest charges accrued while she sought legal help.

Those Pesky Terms of Service: What Happens to the Account of a Deceased User?

As clients create their digital property, they click and consent to the provider's Terms of Services (ToS). Few people read the ToS or know that they have agreed to policies which will apply upon their incapacity or death. Some companies state that allowing anyone else to access your account violates the ToS, further complicating planning for digital property. So you leave a list of passwords to your spouse and he/she violates the ToS by logging in as you. It entirely defeats the purpose.

A handful of states have begun to address the challenges of digital property when the owner becomes incapacitated or dies. One of the most comprehensive laws was enacted in Oklahoma, though it considers only accounts of a deceased person, not those of the incapacitated. It narrowly defines the sites to which the law applies and does not explicitly override the ToS agreed to when the account or site was opened.

Loved ones have been forced into courtrooms to get access to digital property. When Yahoo! refused to permit access to the family of Lance Corporal Jason Ellsworth, a soldier killed in Iraq, they fought back and got a state probate judge to order the e-mail turned over. In another family, Karen Williams found comfort after her son died in a motorcycle crash when she read his Facebook wall. But when Facebook learned of his death, his page was immediately shuttered until she got a judge to reopen it.

It isn't only the ToS you need to worry about. Most providers will argue that the federal Stored Communications Act prohibits turning over users' content. The 1986 Act, while moldy and outdated technologically, remains the law and experts are not sure that state laws could withstand a challenge in light of this law.

A New Dawn

We may be getting closer, albeit slowly, to a solution. On July 16, 2014, the Uniform Fiduciary Access to Digital Assets Act (UFADAA) was approved by the Uniform Law Commission. The Act attempted to balance the need for fiduciaries to get control of digital property without violating privacy promises made by online companies to users or customers and without violating federal privacy laws. Achieving that balance was clearly tough. UFADAA was introduced in 27 states in 2015 and passed in none of them. Only Delaware, in 2014, passed a modified version of UFADAA.

Seeing the writing on the wall, the Commission came up with a Revised UFADAA (RUFADAA), which was approved on July 15, 2015. Seeking to compromise with online providers who opposed the original bill, the new RUFADAA expressly permits the online tools discussed above, making them separate from the ToS and legally enforceable. The online tools would supersede contrary directions in a will, trust or Power of Attorney. If no online tool was used, the will, trust or Power of Attorney would control. If there is no direction online or in a legal document, the ToS would control.

A core provision of RUFADAA allows a fiduciary "the outside of the envelope" – a catalog of communications, but permits the fiduciary access to content only with the consent of the decedent – which could be via an online tool, will, trust or Power of Attorney. Basically, RUFADAA is an overlay statute designed to work with each state's laws. Most experts expect that RUFADAA will be introduced in many state legislatures in early 2016.

A fly in the ointment is the Privacy Expectation Afterlife and Choices Act (PEAC), which Virginia passed in 2015, and which was preferred by many online providers to the original UFADAA. PEAC requires that a personal representative of a decedent get a court order after showing that access to digital assets is in the best interest of the estate. The court can then order that a log of communications (again, the "outside of the envelope") be provided to the representative. Disclosure of content requires the consent of the decedent. This seems to the authors a slow, expensive and cumbersome process. We much prefer RUFADAA.

The State of Estate Planning

As they say in the movies, "it's complicated." We are in a legal limbo at the moment. It appears to the authors that the new online tools are gaining a lot of traction. It may be wise to advise clients to use them, reminding them that, if RUFADAA is passed, those online tools would override other legal documents. Some attorneys prefer to try to address the issue of digital property via a will, trust or Power of Attorney. Court orders in guardianship or conservator cases that include express authority regarding digital property may be appropriate. Agents under powers of attorney can be granted express authority to act for the principal regarding digital assets, to the extent permitted by law and terms of service. Information gathered in an initial meeting intake form should certainly be expanded to include digital property. Consideration should be given to providing a similar grant to agents under medical directives to ensure online medical records are accessible.

Both wills and trust agreements can include language that grants the Personal Representative or Trustee authority to access, maintain, change, or dispose of digital property. As noted earlier, it is not clear whether these planning efforts will be legally effective, but it is far better to attempt to plan for digital property than to ignore it. One thing we would not do – don't notify online providers about a client's death without researching your current state law – and the ToS or online

tools of the provider. In some cases, notification has meant instant deletion of an account. Unsettling? Yes.

Similar to writings often referenced in a will or trust, a digital memorandum could identify the specific property and then for each item provide access information (username, password, PIN) and instructions (delete, preserve, memorialize, distribute to designated beneficiary, sell, or dispose). This type of access is particularly difficult since you need to balance access to the information and the security of the information that is stored; hence another reason we advocate an encrypted electronic file that contains the appropriate access information for all digital assets.

While one can be most diligent in creating a comprehensive list of digital property, that is not enough. The list must be kept current as passwords change and additional accounts are created. Careful consideration must be given to where the list is kept, who knows about it, and who is to have access. There are commercial websites that will retain the information but we question their security – it seems everyone is vulnerable to being breached. Another option is for lawyers to hold the digital property list or digital memorandum in escrow with written terms from the client for the lawyer's release of the list.

Final Words

We have watched attorneys argue endlessly about how to proceed – today – in light of likely legal changes. Because the answer will vary from state to state, our best advice is to make sure you attend CLEs on this topic that are focused on your state – and for heaven's sake, watch legal publications for any indication that your state law is going to change. Whatever you do, now and for all time, digital assets must be part of your estate planning process with your clients.

Authors Nelson and Simek are the President and Vice President, respectively, of Sensei Enterprises, Inc., a digital forensics, information security and information technology firm based in Fairfax, Virginia. In our first look at this topic, in 2013, we lectured with Deborah Matthews, an estate planning and trust and estate administration attorney, who has her own firm, the Law Office of Deborah G. Matthews in Alexandria, Va. We gratefully acknowledge her contributions to our early understanding of this topic.