

Digital Property Planning: A New Frontier

by Deborah G. Matthews, Sharon D. Nelson, and John W. Simek

© 2013 Sensei Enterprises Inc.

A decade ago, there was no Facebook. 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. Much of the world has changed—especially the online world—in the last ten years. Like it or not, it is a new and uncharted frontier. The Internet has profoundly changed our lives and there is no going back. Even those with no desire to enter the digital frontier are being forced there. No longer can recipients of Social Security and other benefits opt to have a paper checks mailed with the U.S. Department of Treasury's all-electronic initiative.

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 Even if we did, technology would continue to morph and our definition would be outdated.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, 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, 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. You may well have licensed them for all of your life, but the licenses typically expire when you die.

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 costly.

Google has forged ahead of others and announced in April of 2013 that users can control how Google Accounts are to be handled if they've been left inactive for any reason. With Google's Inactive Account Manager (IAM), the user can decide the length of the timeout period or how long after the last use the inactive period will start with choices of three, six, nine, or twelve months. Then IAM will send the user a text or e-mail alerts toward the end of the timeout period in advance of the inactive period starting.

IAM also permits the user to name as many as ten people as a "trusted contact" and Google will notify them that the account is no longer being used. The user can also give trusted contacts access to data. This doesn't mean a trusted contact can start sending e-mail as the user. They are not provided with passwords—just data.

A user can also choose to instruct Google to automatically delete all data when the user's specified inactive period

is reached. This addresses concerns some have regarding the user's privacy.

IAM directions apply to personal accounts such as Gmail, Contacts, Circles, Drive, Google+ Profiles, Pages, Picasa, Google Voice, and YouTube but not Google Apps accounts. We love the name "IAM" and the irony that it is intended for use when "you are not."

IAM is on a user's Google Account setting page. For details, see <http://dataliberation.blogspot.com/2013/04/plan-your-digital-afterlife-with.html>.

In this bizarre modern world, you can schedule Facebook, LinkedIn, and tweets to post after you die. Check out the possibilities at <http://www.deadsoci.al/>. The free service claims it will guarantee the delivery of messages for the next 100 years and requires users to appoint a trusted executor. An Israeli site called "If I Die" allows you to send personal messages as well as public Facebook messages and already has 200,000 users. One suggestion the site makes is that you use its services to send all your passwords to a trusted representative after death. The site can be found at <http://www.deadsoci.al/>. A truly strange service is provided by [_LivesOn](http://www.liveson.com/), which uses artificial intelligence to tweet after your death. In one of the weirdest advertising tag lines of all times, the service promises "When you heart stops beating, you'll keep tweeting." It's still in beta testing, but wow, dead people tweeting? And what are the implications for assets that continue to expand posthumously?

A good resource in this area is <http://www.thedigitalbeyond.com/>, where you can find updates on state digital assets laws as well as a list of online services that help you prepare for what it calls "your digital afterlife."

Estate Planning and the Challenges of Digital Assets

The Internet presents new challenges for estate lawyers, who have only recently begun to think about planning for the disposition of a client's personal and business digital property.

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 memo.

Deborah Matthews tells clients not to opt out of paper financial statements. She advises them to toss the statements as soon as they're received, but that way the account won't be hidden. One of her clients bought an old-fashioned address book that her family uses to track accounts and passwords - that is kept away from the computer. Another prepared a list of all accounts, security questions, and current passwords and gave it to her in a sealed envelope with written instructions on when and to whom it is to be released. We recommend the gold standard, keeping data in an encrypted electronic file for security and identity theft reasons, but at least someone is thinking about how to deal with digital assets after death.

Unlike an unknown bank account where a statement will arrive in the mail sooner or later or be found by asking the IRS about reported interest payments, digital property is harder to locate. Once found, it can be difficult, if not impossible, to access. This is true not only for estate planners but corporate counsel too.

Matthews was visited by a young widow after her husband's unexpected death. In their family, he paid bills using online access to their joint bank account. Having never accessed it online, she asked the bank for his password since

she was now the sole owner. The bank refused. She became the court-appointed administrator of his estate and the bank still refused. Unable to learn about the online transactions, she ended up closing the account and having to wait to see what was or wasn't paid — and incurring late fees.

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 ToS. Few clients — or their lawyers — read the ToS or know that they have agreed to policies which will apply upon their incapacity or death. Some companies, such as Google and Yahoo!, 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 then your spouse violates the ToS by logging in as you. It entirely defeats the purpose.

Some 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.

Indiana, Connecticut, Idaho, Nebraska, and Oregon also have digital property laws while Maryland, New York, and North Dakota have such laws pending in their legislatures.

In Virginia, the governor has signed a bill, effective on July 1, 2013, that permits the personal representative of a deceased minor to step into the minor's place for the ToS with providers of Internet services, communications services, or other online accounts to obtain the minor's communications and subscriber records. The provider must give access within sixty days of a written request. A broader bill was withdrawn

after receiving opposition from Google, AOL, and the motion picture industry.

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 commentators are not sure that state laws could withstand a challenge in light of this law.

We have seen many articles suggesting the appointment of a “digital executor” or a “social media executor.” But what good will this appointment do if federal law or a site's ToS run counter to the appointment?

Practical Estate Planning Advice for Attorneys

Attorneys clearly need to address digital property as they assist with estate planning, intellectual property, and corporate matters. Estate planners should discuss who is to have access if a client becomes incapacitated or dies and also disposition of the property at the client's death. 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 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. In Virginia for

example, the commonwealth provides residents with a free online Medical Directive Registry where directives and other medical information can also be stored for later access by health care providers.

In drafting documents, corporate counsel can address online policies in general as well as the incapacity or death of those creating online accounts for the business. Imagine the webmaster of a business dying suddenly without adequate planning for access by someone else.

Both wills and trust agreements can include language that grants authority to the personal representative or trustee to access, maintain, change, or dispose of digital property. As noted earlier, it is not clear whether these planning efforts will be effective in this Wild West electronic frontier, but it is far better to attempt to plan for digital property than to ignore it. If the property is extensive or unique, a digital executor may be appropriate—similar to a literary executor when the decedent is an author.

Without express authority, the personal representative could face significant challenges in marshaling assets of the estate. Leonard Bernstein died with his memoir in a password-protected file so secure that more than a decade later it still has not been accessed.

When a will is probated, it becomes a public document. Many clients wish to keep their financial account information and the websites they frequent private and yet still plan for them. Similar to memoranda or other 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 given the need to balance access to the information and security of the information that is stored; hence another reason we advocate an encrypted electronic file that contains the appropriate access information to any digital asset.

Property owned by a revocable trust is not subject to probate and does not become part of the probate estate or a court file that is open to the public. As with the transfer of tangible personal property to a trust, ownership of digital property could also move to a trust. A very cautious client could pursue creating digital accounts as “trustee” of her trust.

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. 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 may be getting closer, albeit slowly, to a solution. In February of 2013, a panel of the National Conference of Commissioners on Uniform State Laws met in Washington, D.C., considering a draft of a “Fiduciary Access to Digital Assets Act.” The Act attempts 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 could be tough.

As we go to press, the first reading of this draft is expected in July of 2013 and the final reading in July of 2014, with passage anticipated in the fall of 2014.

No one knows where the legislation being considered at the state and national levels or potential changes to ToS will end up. We are all playing the digital roles of Lewis & Clark in uncharted territory. As you may recall, they once stood at the fork of a river and simply had to decide, without benefit of a map, which way to go. We now stand at a place in our digital river which has many forks, and the right way forward is not clear.



Nelson



Simek



Matthews

Sharon D. Nelson and **John W. Simek** are the president and vice president, respectively, of Sensei Enterprises Inc., a digital forensics, information security, and information technology firm based in Fairfax. **Deborah G. Matthews**, an estate planning and trust and estate administration attorney, has her own firm, the Law Office of Deborah G. Matthews in Alexandria. The authors thank Ellen E. Mains, George Mason School of Law, class of 2013, for her research assistance.