Digital Death

Purgatory for the Unplanned Decedent?

Philadelphia Estate Planning Newsletter – April 2014

By Holly Isdale
www.digitaldeath.com

At its essence, the process of estate administration can be distilled into three simple steps: (1) **inventory** the assets of the estate, which requires the executor or fiduciary to identify the assets, ensure control the assets, then preserve or curate these assets during the period of the administration, (2) **value** the assets as of the date of death or the alternate valuation date, and (3) **transfer** the assets in accordance with the estate plan or appropriate laws.

At the risk of waxing nostalgic, this process, even when complicated, used to be a lot easier. When someone died, the family and the executor could easily find the assets – they went through the file cabinet or desk drawer and pulled out the checkbooks, looked for the old utility bills and maybe opened the safe deposit box at the bank for some papers. Perhaps the executor had to sit by the mailbox to watch for forgotten accounts or to clip the coupons on a bond or two. Today, however, the only thing that comes in the mail seems to be catalogs or store circulars. As we buy, sell, consume and communicate online – our correspondence is often virtual, our receipts and records are stored in a number of places but generally not in physical form.

Consider this: If you had died last night, instead of being able to read this article, would your spouse, your partners, your clients, have been able to access the information needed to inventory, value and transfer the digital assets of your estate?

The average household has six or more Internet connected devices, upwards of fifteen or more in wealthier homes. College students alone average about seven devices. Over 91% of Americans use cell phones, many of whom (34%) use it as their primary access to the Internet, forsaking computers (archaic!) or even tablets (passé!). Want to track down a decedent's bank accounts? Better have clear authorization in the appropriate documentation AND their email (the average American has upwards of six distinct email accounts), the right passwords, and the verification information, especially since 61% of Americans now do their banking online, and at least 30% of those use cell phones exclusively for banking transactions. Oh, and by the way, it's considered a criminal offense under several federal laws to use someone else's login information -- to further complicate the process, a normal power of attorney is not considered sufficient authorization to grant online access.

What are Digital Assets and Why Do We Care?

The Uniform Probate Code defines "property to include "both real and personal property or any interest therein and means anything that may be the subject of ownership" (Unif. Probate Code §1-201 (38) (as amended 2010).) With digital property, nature of the asset is constantly changing and evolving. Digital assets can include the obvious items such as hardware (computers, tablets, cell phones), memory devices (thumb drives, CDs, floppy disks, etc.), software programs and the content from these programs. However, digital property goes beyond tangible assets to include both the method of creation (those six email accounts for example), as well as the content of those accounts (the emails themselves) and can include the manner in which they are stored or the data attached to the digital asset that can prove when it was created, amended (the "metadata" tags). As the average Internet user, in addition to multiple email accounts, has photos stored online or digitally, music, videos, social media accounts, instant messaging, messages or communications within social media accounts -- the list can start to spiral out of control. Eric Schmidt of Google postulated in 2010 that if we took all of the data created – all information, all human knowledge, from the dawn of time to 2003, it would amount to about five Exabyte of data (each Exabyte is a billion gigabytes). We now create that same amount of content every two days – mostly in user generated content such as photos, messages, social media posts, chats and blogs.

While most of the content on our various digital devices may not have huge monetary value, it is important for the fiduciary to understand the extent of the content, and whether it has commercial or personal value, and then to preserve that accordingly. If you flip through your own devices, you would be surprised at the number of applications that either contain content or provide access to user generated content, browsing history, medical or personal information.

Gaining Access

Once you have identified the assets, you need to ensure access and control over them. Passwords change rapidly, the average American has at least ten distinct passwords with more technologically connected individuals having upwards of 35 unique passwords. Each of these can have verification cues that need to be approved (is this the right picture for your account?) or answered (what was your high school mascot?). For more secure sites, passwords must be changed frequently and may require authentication devices, which now can be an app on your cellphone that generates the PIN you have to input to gain access to the website or content. Even if you are able to access a site because the decedent thoughtfully left you an updated list of passwords, with all the verification and authentication, and what email gets the reset links if you try to reset the account, there are at least three federal laws prohibiting your use of these passwords or preventing the service provider from releasing information. The Stored Communications Act (18 USC Sec 2701 et seq.), part of the Electronic Communications Privacy Act of 1986, contains two provisions limiting access, the first makes it a criminal offense to access a facility on which an electronic communication is stored without having the proper authorization from the user and prohibits the voluntary disclosure of customer communication and records by a service provider. Separately, the Computer Fraud and Abuse Act (CFAA) prohibits the unauthorized access to computers and provides penalties for exceeding authorized access as well. In addition to the federal statutes, states have enacted similar provisions either limiting access or imposing penalties, all with an eye to preserving consumer privacy. Many states are now enacting legislation to permit access for fiduciaries but the level of access is uneven (access to emails only in one state, access to records but not communications in another) and since the federal laws remain intact, large providers (Facebook, Yahoo, etc.) have been successful preventing the release of data in lawsuits by executors and estates seeking information, because to release the information would be a breach of the CFAA or the Stored Communications Act.

The Uniform Laws Commission has established a committee on digital assets that is finalizing a proposed Uniform Fiduciary Access to Digital Assets (UFADAA) model act to be published later this year. UFADAA, if enacted at the state level, will remove many of the federal barriers to access and remove the criminal penalties for fiduciaries seeking access. However, the model act is designed to apply only where the fiduciary, conservator, agent or personal representative has affirmative, written authorization to access the data under the terms of the relevant documentation (power of attorney, will, revocable trust, etc.).

How to plan in uncertainty?

If UFADAA is enacted, it will still require the written authorization for the representative to access data. As such, and in the absence of clear laws, it is important to incorporate language in wills, revocable trusts and powers of attorney that address digital assets and authority to access these assets. The language should be broadly written, and recognize the changing nature of assets and the decedent's intent to capture assets that may not be contemplated at the time of signing. At the same time, it is important to clearly provide the representative with the power to delete or destroy data, and to vest in them the ability to do so without repercussion. Not every estate warrants an archivist to sort through email communications and pictures posted on Facebook. However, it is important to understand what might need to be preserved for posterity and what should be deleted. Some practitioners prefer to establish a separate digital executor or trustee, who can address these issues apart from the regular administrative actions of the trustee or executor.

There are a few practitioners advocating the use of "digital asset trusts" to hold title to digital assets, however the TOS contracts often prevent the transfer of these assets as the licenses granted are single-user, non-transferable licenses (next time you log into Amazon or iTunes, take a moment to read the fine print!). Few service providers have incorporated provisions in their contracts dealing with death of the initial user, and the ability to access, and transfer assets can be further impeded when non-US companies are involved. Best practices would indicate that including specific digital language into wills, revocable trusts (which have greater flexibility in times of disability than powers of attorney when it comes to the terms of service agreements with various technology providers as well as most financial institutions) and to have clear authorization in powers of attorney as well. Some commentators recommend broad stand-alone authorizations for digital access but it seems more prudent to tie the access into a more conventional legal document where state laws as to the revocation of authorization (such as laws governing the revocation of a power of attorney) would govern.

Finally, all HIPPA documentation should include language clarifying the authority and access to medical and health information after death. The HIPPA statute clearly contemplates the post-mortem control of medical records; indeed, the 2013 changes to the statute reduced the privacy to 50 years post mortem, as opposed to the perpetual restrictions on this information in the original statute. Aside from some public policy exceptions, the person holding the HIPPA power, or the executor or personal representative, has ultimate authority to disclose or withhold medical information. For blended families, or same sex marriages where state-law conflicts may arise, it is important to clarify an intention to share medical information or health records. The surviving spouse may not need or care about the information to the same extent that a biological child would benefit from knowing when and how a parent's health declined or when certain treatments were tried. For some families, ensuring access to a decedent's medical history might be the most enduring legacy they provide, if it would allow for earlier detection and treatment of diseases in their descendants.

What are your tweets worth?

Once the executor or trustee has identified and accessed the assets, the question of value comes to the forefront. Most of us would agree that the value of our hardware devices is *de minimus* compared to the information that is contained on them or accessed through these devices. A recent survey showed that people would value their digital assets at about $55,000 – which may seem low in terms of sentimental value of emails, photos, social media posts. While sorting through endless emails or pictures of cats downloaded off of the internet, is not a great use of time, its clearly important to know where valuable assets are held – there are numerous stories of people finding cash in online accounts they forgot they had or recycling hard drives that contained important documentation, or Bitcoins, without checking the hard drive first first. Clearly business assets, such as domain names, websites, newsletters, blogs or other content, have a value and this value can change over time if not maintained. For these assets, the alternative valuation date might be appropriate but the executor or trustee will need to be aware of their own liability to understand and implement actions necessary to preserve the value of the assets during the administration period. Finally, even simple things, like travel pictures, can be monetized and the executor or fiduciary will benefit from releases in the relevant documents, exonerating them from having to find possible value all assets.

(Note, however, that there are some companies forming to help monetize the value of online gaming assets, where picking up a special hat or sword in an online role playing game, can be worth several thousand dollars! Lest you think your teenage son is simply frittering his time away online – there is gold in those virtual worlds!). Strong release language in the documents, providing relief to the executor and permitting them to abandon digital assets, or affirmatively delete assets, should be incorporated into any standard digital language templates.

Finally, if transferable, the asset transfer must be done properly, which can require multiple steps depending on the asset. For many assets, the transfer is technically not permitted, but what liability accrues to the executor who transfers a Kindle, iPad or other device containing the decedent's electronic books and music?

What's the rush?

For some clients, turning to the digital assets a month or so after a death may be sufficient, especially if they were not very technologically. Unfortunately, this may not be a wise delay, even if the executor believes that the situation is not pressing. Some email service providers will disable accounts after a relatively brief (60 day) period of dormancy. More importantly, the decedent's digital life may have been very connected to his financial one. Online magazines and subscriptions can automatically renew without anyone noticing, especially if these, like many online accounts with eBay, Etsy, Amazon, are connected to PayPal, which directly debits the bank accounts and, if the accounts run short, automatically rolls to credit cards (risking personal liability to the fiduciary or executor if they fail to control or protect the asset). Further, identity theft of the deceased is on the rise, particularly because the family and executors tend to take a few months to turn to the online accounts, giving thieves the opportunity to establish new credit cards, obtain identity papers and perhaps deplete bank or other accounts. As such, its better to err on the side of caution and establish control over the assets as soon as possible.

Beginning the discussion with clients today about digital assets is a good first start. Once they understand the scope of the problem, most become very focused on ensuring that they have records and directives in place. As a first step, all clients should be encouraged to inventory their digital assets and create records of passwords, login verifications and note what email accounts are tied to these various assets (does your bank account reset to your Apple account or your Gmail account?). They should try to maintain these inventories on a regular basis. I prefer to do "pre-death" audits with all clients as a matter of practice – running through the asset values and specific accounts that will transfer to various beneficiaries upon death. In some instances, we have taken these through to include dry runs of trust issues ("in this fact pattern, should Jack get a distribution for a new business venture?"). Incorporating the digital discussion into these audits can prove quite eye opening when you begin to realize the potential value of domain names, client lists, email addresses or online gaming avatars. All practitioners should begin to incorporate digital language in their documents and increase the use of revocable trusts in case of disability to ensure access (if not for general ease of administration of the other more tangible assets).

For more information, or copies of sample documents, go to www.digitaldeath.com

As of April 2014