DIGITAL DEATH

Preparing a Digital Assets Inventory

A key requirement to managing your Digital Assets is to have a comprehensive list of exactly what assets exist. Unlike your physical assets, its not that easy to find your online account information and without the proper authorizations, most providers are not required to even reveal the existence of these assets to a legal representative, executor or trustee.

An inventory can take many forms. There are several planning tools and worksheets available (including our own Digital Asset Inventory) but for many people, a simple trigger list is better than asking you to fill out forms that merely repeat information that is found elsewhere. Not only is this time consuming, its not an efficient process as the information can change frequently. We recommend using a "trigger list" combined with whatever system works for you to identify and maintain the data you collect. For some clients, this is excel or a word file, for others, it's a spiral notebook and a pen.

Regardless of what system you use, the purpose of this inventory is to create a comprehensive list of your digital assets and to maintain this list in a convenient, yet secure, location. We have had some clients complete their inventory entirely from memory while others choose to work on it over a period of weeks, usually wandering around their home looking for items or flipping through credit card statements to identify overlooked charges. Obviously the more technologically connected you are, the more items you will have to list!

It is important to be as thorough as possible in making the inventory, although any progress is a good start and may spur you to think about your digital assets differently. Don't forget to include old items languishing in cabinets, drawers or closets (and maybe its time to think about recycling those anyway). For all entries, ask what other information is needed – do you need to know payment information, where backups occur, etc.

If you have business or professional assets, it's worth having a separate list of those or noting where business and personal assets are mixed (files on a hard drive, for example) and suggested directions for dispositions or issues that may arise as to where items should go after your death.

Your inventory should be stored in a safe location, updated at least annually and its existence shared with your advisors and family, as appropriate.

Hardware

Computers or Laptops: List the make, model, passwords, and location for all items. Consider adding notes as to information or file organizational structure if possible. If you know where the software licenses or service contracts are, include this information as well. Note what should be recycled, what needs to be deleted, and any recommendations on service providers if you have a local

> **A word on file structure: If you are like most people, your computer files are a random assortment of files, dates and topics. It is worth taking a moment to create some type of consistent organizational structure around the data you have, even if its lumping everything up to now in an "archive" file and starting anew. It will make it easier for you to maintain information as well as to find items. While you may know the keywords to put into your computer search to uncover the supporting documentation to your 2012 tax returns or the letter to Aunt Jenny, your executor or trustee will not.*

Tablets: Include the make, model, passwords and (last known) location. If the device has GPS locator features, note how these are accessed. Consider listing the most commonly used apps on the tablet and any passwords or account numbers for information stored there. (Magazines in particular are often on auto renew and can pile up on the online app without anyone noticing!). Include here, and note any linked online accounts, such stand-alone items such as Kindles, Nooks, other e-readers, mp3 players (Zune, anyone?), Garmin or other navigational devices, etc.

Smart Phones: List the make, model, passwords, and likely location. Include information on the service contract, renewal information, as well as instructions to access any online service account (including online passwords, PIN and verification information as well as the account numbers for the service provider and a contact number, not a website, if possible). Include a listing of apps and information. Also worth noting what computers or cloud-based backup is used to store the information on your smart phones.

Peripherals: For storage or back up devices, note the make, model and serial numbers, as well as service contracts and receipts. Note also what computers link to what backup systems. For smaller devices or storage media (external hard drives, thumb drives, CD-ROM, and other information), note the relevant information and location. It is a good practice to routinely clean off any storage devices used for information transfer (thumb drives, etc.) and to dispose of these properly.

For all hardware, note any specific disposal or cleanup instructions (delete files, save information), what information might be located on the system that would be helpful for income or estate returns, is sensitive client information or personal data and what should be deleted. Service contracts, receipts, and related information should be noted as well.

For encrypted information, encryption keys, information as to resets and any supporting documentation is important.

Software:

For software *uploaded* on computers, laptops or tablets, note the computer where the software was loaded and the version, location of the actual software disks themselves and the licensing materials and any information necessary for reloading or transfers (passwords or other keys).

For software *downloaded* on the various devices, note the download date, account numbers, password, verification information and access restrictions. For example, some software is linked to an encryption key application on your smart phone, requiring smart phone access to change or access software.

File Storage:

In addition to the information compiled during the inventory of your hardware, create a list of files or information that is stored electronically in the cloud. It is more important to provide guidance as to how to reset passwords than to maintain an up-to-date listing of the most recent one, as these change frequently. What email accounts do you use as the reset account? Does it require a PIN that is sent to a home phone or cell phone? If these were Provide a summary of passwords, usernames, billing information and other access or account information as well as where and how these were commonly accessed to ensure that backups are maintained. Some common storage locations might include Dropbox, Evernote, Box, Apple iCloud, Google Docs, etc.

Do not forget documents that may be stored in online "vaults" with financial institutions, attorneys, accountants or other advisors as well as personal cloud based systems. Include in your inventory as well things like online photo storage sites (Flickr, Tumblr, as well as photo printing sites (Shutterfly, etc.) where you may have uploaded photos for albums, holiday cards etc., any online receipt management (Shoeboxed) or budget sites (Mint, etc.) and similar items pertaining to other areas of your life. Systematically review your bookmarks, apps and other files for additional triggers as to possible places where information may be stored. Note also that your email, receipts, calendar, and related information will be important for your final income and estate tax returns. Try to capture as much of the online information as possible and create a checklist as to what information needs to be deleted, saved or might have relevant financial or personal significance. **Of particular importance is to note any automatic payment features, auto-renewals, passwords, login and verification information for these online files and the attendant service providers.**

Digital Footprint: You have left marks on many areas over the Internet. If important, review blogs where you may have posted, information you have shared and consider what needs to be removed (now or at your death) and make notations. Is it important to have your Weight Watchers information or should that account be removed – at a minimum, the auto pay needs to be disabled!

For all of these areas, you should have the user name, password, account information, verification information and any other identification mechanisms logged as well as directions as to content or continuity for the site. Note which should be disabled and what information should be archived or deleted. For many people, you may just have a long laundry list of "turn off or delete the following apps" and be done with much of the following.

For your digital footprint, be sure to fully catalog the following types of information:

Financial Data: List all bank accounts and financial institutions, including email address, password, verification information, security questions (noting in particular any capitalization or alpha-numeric patterns) and encryption keys (and access thereto). Don't over look other financial accounts such as brokerage or perhaps other online investment accounts as well as any financial planning or tracking accounts such as Quicken, Quickbooks, Microsoft Money, etc., and tax preparation software you may have used in a cloud-based application. Do not forget to provide access and passwords to other providers, such as Paypal, and firms like Coinbase, etc., which might hold your Bitcoins or virtual currency information.

Be sure to capture retirement benefits, pension, or other information as well, for former employers. If you are not old enough to claim the benefits, your estate or beneficiaries may be entitled to claim these funds. For this, they will need contact and account information but also may need your employee identification numbers or dates of service.

Credit Cards: For all credit or debit cards, maintain the physical contact information as well as the online web address; customer service phone number and PINs are important as well. Many times these cards get cut up or destroyed after death only to find out months later that your executors needed the PIN on a card that was destroyed to turn off an auto-pay function or to access an account. **Many times powers of attorney are not sufficient to access online information for credit or bank accounts!** It is worth the executor enrolling a decedent's social security number in a credit-monitoring agency for at least a few years after a death to watch for credit scams and to ensure all old accounts are closed.

For all credit cards, as well as financial institutions, note if you have received perks or benefits (a free safe-deposit box, frequent flyer miles or other points) that should be cataloged as well.

Utilities, Service Contracts and any other non-financial Financial information: There are many accounts which should be addressed so consider utilities, service providers or service contracts that may be on auto-pilot and provide contact information, account numbers and access instructions. Gas, water, electric, etc. are all important to keep running for maintenance of a house, but also lawn service, pool service, sewer and other maintenance features. Don't forget to provide your home security account information, access codes as well as online passwords, account PINs and verifying information. Remember to catalog online accounts like Hulu, Netflix, YouTube and others where you may have auto pay features or account credits.

Don't forget frequent flyer or frequent buyer accounts, where miles and other points can be transferred and consolidated.

Email Accounts: You may use a central system (Outlook, Mac Mail) to access your various email accounts but its important to have a list of all email addresses, even dormant ones, with passwords and access information (verification, security questions, linked accounts where resets may be sent). Common ones are Yahoo, Google, iCloud, of course, but don't forget the "spam" accounts you may have set up for use on internet sites, or accounts you have "in perpetuity" from schools or universities where you studied. Note also if there are aliases used in accounts or older logins (for veteran Apple mail users, we have @mac.com, @me.com and @icloud.com appendages to our emails). Include information as well if you have administrative capabilities on email groups or list serves, especially through Google Apps and other services or need to be removed from these services. Note if there are addresses or usernames, which may have value from a personal or corporate brand perspective or might be "interesting" to other people (unusual last name, short or catchy address).

Social Media or Social Networking: The list here is endless but think through what you are likely to use frequently -- Facebook, Twitter, LinkedIn, Google Plus, Foursquare, Instagram, Vimeo, Vine, etc. In addition to including the information suggested (usernames, avatars, etc.), note whether there are addresses or usernames, which may have value from a personal, or corporate brand perspective or might be "interesting" to other people (unusual last name, short or catchy address).

IM, Chat or Video accounts: Skype, Facetime, MS Messenger, AOL IM, Google Talk, etc. Include Google phone, Line 2 and other communications services in here.

Gaming Accounts: For gamers, the account information, avatars and "assets" of the accounts can be significant. Note specific assets and distribution provisions if necessary. While there may be little monetary value, perhaps that special sword you collected on Steam, might be transferred to an online gaming pal. There are companies that specialize in helping to monetize assets here. In particular, if your gaming accounts are linked to Paypal or financial accounts, note this and provide instructions to disable the link (after any monetization might occur perhaps…). Gaming is not limited to your World of Warcraft account. Consider the various puzzles or other apps on phones and tablets, what information or credits are in the apps and what payment accounts they may be linked to as well as emails for resets.

Merchant Accounts: Information stored online for merchant accounts can be incredibly helpful to establish the cost of items purchased, as well as service contracts or warranties on items. Be sure to note your account information as well as emails used to access the accounts (incase passwords need to be reset) and what might be relevant information on the accounts. Common ones are Amazon, Ebay, Paypal, perhaps Craigslist or Etsy. If you are a merchant, you will have items of value, which could include your reviews, your selling ratings and perhaps brand names for "virtual storefronts." From a business succession

perspective, it is important that someone is monitoring these accounts for orders and that online sales functions are attended to, or shut down, in a focused manner.

Password Sites: There has been a proliferation of online password sites that can track your passwords or even provide access to passwords to your trustees or executors. We believe these sites may be useful for some individuals but do not take the place of a full review and summary of the digital assets they possess. Further, the security of these sites remains subject to debate and any information, whether stored in physical or electronic form, should be suitably protected from theft, loss or destruction. If you do use a password "keeper" or tracking site, be sure to have the information for that website cataloged and be sure to check their terms and conditions on access to the site and information in the event of your demise.

Websites and Domain Names: For online content or sites, be sure to note the hosting provider as well as the registrar of any websites and domain names, including domain names you may have bought for future use. Include passwords, account information, contact information (websites and phone numbers) and any other relevant information. Document if possible the purchase dates and transfer information around the websites and domain information. Provide guidance as to the disposition of content (delete, backup, sell, preserve) if possible. Consider as well what content you have on other sites (YouTube) that should be inventoried and administered.

Regular backups of information are important to keep this list current. At a minimum, you should review it annually, update passwords as frequently as possible and ensure that a spare copy of the information is stored offsite (or online but securely) so that it remains available in an emergency. While I have had many clients do complete inventories of real and digital assets, only a few have passed away where the inventory is handy. For others, the information proved vital for insurance claims with storm damage or theft, so this exercise, while overwhelming, can be very worthwhile!