Chapter 6
Your Digital Estate and Digital Assets

While writing this book, my family had the happy opportunity to celebrate my father's 100th birthday! About 50 family members attended the party and shared stories about this exceptional man! He was born in 1917, and one can only wonder what life was like for him, experiencing all the technological advancements that have been achieved over the past hundred years!

He was born long before the Internet; before computers, smartphones, fax machines, beepers, cable, television, air conditioning, and even before permanent press!

Until the invention of the computer about 40 years ago, pretty much everything you needed to know about someone else's assets, documents, life, or information of importance could be stored and found in a file cabinet, photo album, box in the closet, garage, attic, or storage locker. Everything had a tangible, physical form.

Books were on shelves. Photographs were in an album. Phonograph records and audio cassettes were kept near the phonograph or tape player. Family movies, and later family videos, were kept on a shelf or in a box, somewhere they could easily be found.

And important documents were in a filing cabinet, drawer, or stored with your lawyer, accountant, or elsewhere in physical form.

If you needed an address of someone to be contacted, you only had to locate the person's address book.

You might have had to search through a lot of places to find needed information, but a room-to-room search eventually revealed most of what one needed to handle the affairs of a loved one.

If the person wasn't good about saving or organizing records such as bank statements or insurance policies, you could simply wait for the mail to be delivered, and over the course of a year or less, by reviewing the incoming statements, bills, and mail, you could determine where the person banked, what accounts he or she had, what investments, annuities and insurance policies existed, and figure out what assets were owned. Similarly, you could figure out their debts, loan payments, insurance premiums, and other important bills which needed to be paid.

Now, 100 years later, most of the foregoing information is stored digitally, either on the hard drive of a computer, on some digital storage device, or stored online in the "cloud." Banks encourage their depositors to "go green" by having statements delivered digitally to their email address, rather than kill trees and send paper statements. County tax collectors now issue digital automobile Certificates of Title. Income tax returns can be filed with the Internal Revenue Service electronically. The use of paper documentation of information of importance has become less prevalent than ever before, which can cause complications if your loved ones don't know sufficient details about your financial affairs.

If your loved ones don't have actual knowledge about your assets, debts, insurance policies, or where your important documents are stored, there is a strong possibility they will <u>never</u> be able to find information about them. And even if they know where the information is located, without knowing your username and password, they might not be able to <u>access</u> it.

Some digital assets have obvious financial value, such as online bank accounts, Bitcoin or other virtual currencies, etc. But often, one neglects to include websites, domain names, online stores, and other digital accounts as assets having potential value, sometimes significant value. These assets need to be disclosed to your loved ones, and in many cases, should be included in one's Trust and/or Last Will and Testament.

Your legal documents should grant authority to your trustee (in your Trust), Personal Representative (in your Last Will & Testament), and attorney-in-fact (in your Durable Power of Attorney) to access, maintain, and legally do whatever is necessary to administer your digital assets and data.

Most states have enacted some version of the Uniform Fiduciary Access to Digital Assets Act, which gives Internet users the power to plan for the management and disposition of their digital assets. Be sure to check with your estate-planning attorney to verify whether your state has enacted it. In addition, be sure to have your attorney include language in your estate-planning documents granting your fiduciary representatives the legal authority to access your digital assets and manage them.

And watch out for the *Terms of Service Agreements* (TOS) you need to "click" before using when you access certain websites or internet content. The TOS provisions are usually contained in a pop-up box which require you to scroll to the bottom of before you can click the "I accept" box and use it. I don't believe I have met more than three people who admit to taking the time to read what they have agreed to by checking the box, but when you click it (and you won't be granted permission to use the website without clicking it), the TOS content restricts your rights to access, use, and control the content of what you have posted to, or accessed on, their site.

Different states provide different remedies and orders of priority regarding your rights to these digital assets, as to whether the Terms of Service, the Uniform Fiduciary Access to Digital Assets Act, or your own legal documents take priority in granting you the authority needed regarding these assets.

Using your email address as an example, once you have determined which grant of authority applies to your situation, each email provider usually has its own set of requirements on how your representative, assuming one has the legal authority to do so in the first place, can manage your email accounts after your death. On their website, Everplans™ lists the requirements imposed by Gmail, Yahoo, Microsoft Hotmail and Outlook, AOL, iCloud, etc., and the differences among them are quite significant.

The term *"digital assets"* encompasses a wide variety of assets we now commonly use, and the number of type of digital assets is growing as fast as the imagination of their developers can create them, especially as the power, storage, and processing speed of the devices that use them increase.

According to the digital asset management company, Everplans™ (www.everplans.com), digital property can be broken down into three main categories:

1. **Personal digital property**, which includes:
   a. Computing hardware, such as computers, external hard drives or flash drives, tablets, smartphones, digital music players, digital cameras, e-readers (such as the Amazon Kindle™), and other digital devices, including the content you have stored in the devices
   b. Online accounts, including email addresses, social media, photo and video sharing, shopping, video gaming, and online storage accounts, as well as websites and blogs you manage, including content you have written or posted to these sites
   c. Information or data that you have stored electronically, including online storage, cloud-based storage, remote storage, or physical storage devices
   d. Domain names; and
   e. Intellectual property, which includes copyrighted materials, registered trademarks, patents, and any code you may have written and own

2. **Personal digital property with monetary value**, which includes:
   a. Computing hardware
   b. Websites or blogs that generate revenue for you
   c. Art, photos, music, ebooks, intellectual property, or other digital property that generates revenue for you

d. Accounts that are used to manage money and may hold money or credits (e.g. PayPal, Bitcoin, etc.), online bank accounts, loyalty rewards programs, and other accounts with credit balances for your use
e. Domain names

3. **Digital business property** may include:
   a. Online accounts registered to the business
   b. Digital property owned by a business organization
   c. Online store assets, such as your own online store or other sites through which you sell things (e.g. eBay or Amazon)
   d. Mailing lists, newsletter subscription lists, email lists of your company's clients; and
   e. Any client information, including customer history

You are encouraged to make a list of all your digital assets and how to access every one of them. Without this information, access to assets and essential information may be lost forever. There is a section in the attached Questionnaire which breaks down your digital assets into the following categories:

1. Master password programs
2. Email accounts
3. Social media accounts
4. Websites, blogs, and copyrighted materials
5. Gaming, entertainment (i.e. Netflix, iTunes), subscriptions (such as magazines), family sites (e.g. ancestry.com)
6. Online storage or backup sites
7. Digital devices (e.g. computers, cell phones, tablets, etc.)
8. Financial sites (e.g. bank, insurance, investment account, 401(k), Bitcoin, etc.); and
9. Miscellaneous sites you visit (e.g. your doctor's office, monitoring your home security system, etc.)

If you haven't made an actual list yet, start doing so. If needed, for a month, every day for a month (or longer), every time you access a website you use, particularly those relating to your business or containing information you want your loved ones to know, write down the website address, your username and password, any security icons, pictures or phrases, and challenge questions.

Obviously, this is highly confidential information, which will give anyone in possession of it the ability to access your websites. So, either consider using a password manager program (and share only the access information to that account, rather than the passwords to all your sites), or make a list, such as the one contained in the "My Everything File" questionnaire.

Once you have compiled the list, you will need to decide what you want done with these digital assets. Different assets may need to be handled differently from one another:

1. Archive and save the assets
2. Delete or erase the assets
3. Freeze the assets
4. Transfer assets to family members, friends, or business colleagues
5. If assets have monetary value, you will need to decide whether to shut down the site (such as an online store), transfer revenue-generating assets to someone else (e.g. websites you manage), and whether credits, points, or cash values should be redeemed

You may also want to consider naming a Digital Executor to handle your wishes regarding your digital assets. This is not currently a legally binding or enforceable designation, such as the Executor of your Last Will and Testament, but it is a useful method of carrying out your preferences regarding assets which are usually not part of your Trust or probate estate.

The Everplans™ website also mentions something almost nobody ever thinks about, namely identifying potential "skeletons" in your closet." This is information or paraphernalia you wouldn't want anybody else to know about, both digital and nondigital, such as websites you would be embarrassed for your loved ones to discover. You can name someone whom you trust **implicitly** to serve as a "**Cleaner**," who would have the authority to delete your browser history and cookies on your computers, locate and delete offending files on your computer and external backups, drives, and other storage media, delete emails and social media postings (or entire accounts), delete pictures and texts on your smartphone, dating or adult websites, digital help or support sites for abuse, addiction, etc., and potentially offensive tapes, DVDs, magazines, photographs, toys, weapons, diaries, narcotics, criminal record, secret society membership, and anything else you want to permanently dispose of when you are gone.

Since this book is not intended to be comprehensive resource regarding digital assets, I have included only the most basic of information. For additional information, check out these sites which discuss digital assets, your digital estate plan, and your digital legacy at greater length. Providers of these sites state that they maintain secure digital storage of your important documents and information.

Disclaimer: As stated elsewhere in this book, as a senior citizen, I don't completely trust the safety and security of anything that is stored on the Internet, but I confess this to be a personal bias. Hopefully, providers of these sites are correct regarding the security of your information stored there, but please do your own due diligence regarding storage of confidential digital data.

Everplans™ www.everplans.com
This website provides digital asset management and document storage, much of which is discussed in this book and questionnaire. Their website contains a wealth of information about digital assets and their use and management when you are gone.

Mylennium Digital Executor Services www.mylennium.com
Their website has a very user-friendly online Digital Estate Assessment Questionnaire, which helps you to identify which types of digital assets you use and what may be needed to create your own digital estate plan. This digital estate plan includes:

1. Personal and business email addresses
2. Digital devices you use
3. Devices on which you store documents, photos, and videos
4. Websites on which you store documents, photos, music, and videos
5. Social media websites
6. Online genealogy websites
7. Digital legacy websites to store digital assets
8. Personal or business blogs
9. Electronic address books
10. Subscription-based sites for online services or products
11. Online banking, gambling, crowdfunding, gaming, and virtual currency websites
12. Professional or business sites you own, sell products, or manage for others
13. Domain accounts you use
14. Backup, storage, websites; and
15. Much, much more

There are numerous other websites and software applications relating to Digital Asset Management (DAM), so I encourage all readers to learn as much as they can regarding this ever-expanding field, as it has a significant effect on our assets and our use of those assets, as well as how our loved ones will be able to use those assets.