

Estate Planning for Your Digital Assets

By Dennis Kennedy

March 2010

Given the wealth of information we have housed on our computers and the Internet today, smart estate and succession planning includes addressing how to handle digital assets.

Andy Olmsted was a rare individual, in no small part because he is one of the few who thought carefully about what would happen to his online presence if he were to die. A popular blogger, Olmsted wrote a post before he left for service in Iraq, along with instructions for his survivors to post it to his blog in the event he was killed in action. Unfortunately, it had to be posted. I read the post on the day it appeared in 2008, and I re-read it when I prepared to write this article. It remains for me one of the most moving posts in the history of blogging http://obsidianwings.blogspot.com/obsidian_wings/2008/01/andy-olmsted.html.

We are gradually, and grudgingly, learning that our online presence can outlive our physical presence and possibly even take on a life of its own. As we begin to move more of our activities—financial, social, work, leisure, creative—to the Internet, the questions about what happens to our online presence and how we best prepare to handle that have begun to grow in quantity and complexity.

Initially, as the Internet gained popularity, we realized that a person's Internet presence could raise a few important issues in the event of death or incapacity. For, example, what would happen to an e-mail account? Who could access e-mail messages? Were there online financial or other accounts? In the earlier days, our online presence was just a small part of our "digital estate." Today, though, we leave a wealth of information on our computers and on the Web, and our "digital estates" have begun to raise a number of complex issues.

At the root of many of these issues we find the question of passwords. In simplest terms, how can you log on to someone's computer to do anything if you don't have passwords? And once you logged on, you might well confront a different set of passwords for e-mail and other online accounts.

Also, in a relatively small number of cases a few years ago, someone might have a Web site or other Internet vehicles, like listservs or discussion groups. Issues might include deciding whether and how to notify audience and friends of a death, tracking down financial accounts and determining how to shut down a Web site. Yet as difficult as those issues could be a few years ago, they can seem simple in comparison to the myriad issues we see today, especially in the online world. Examples include:

- Multiple computers, flash drives and iPods
- Blogs, Facebook accounts, Twitter accounts and multiple e-mail accounts
- Photos on Flickr, documents in Google Docs and videos on YouTube
- Online bank and investment accounts, online medical information and subscriptions of all kinds

- Myriad online shopping accounts that might hold credit card information, subscriptions and memberships, and many “Web 2.0” services

It's difficult to know where our survivors would start, other than that they would likely be overwhelmed. Therefore, planning for digital assets is becoming part of good estate planning and succession planning.

Basic Planning Concepts

Conceptually, the same principles apply to planning for our digital assets after our demise as apply to our real-world assets. Yet handling digital assets can quickly become quite complicated. Most of us keep important papers, necessary information and valuable assets in safe places. These places are usually revealed to a few trusted people who we hope also survive us. On occasion, though, family members will be surprised to find unknown accounts, collections or even boxes of cash. However, it usually takes a simple conversation, a page or two of notes, and pointing loved ones to the file cabinet or box where the important assets are kept to handle 90 percent of the issues.

In comparison, making arrangements for digital assets can be an order of magnitude more difficult than making arrangements in the physical world.

Take a moment to do this mental exercise: Can you quickly and easily find all the valuable documents and files on your computers? Or, as is likely, are they scattered among many folders, several computers, flash drives and backup CDs, DVDs or tapes? How easy will it be for someone to sit down at your computer and find everything they need, especially if it's now a struggle for *you* to do so?

Add to that the simple fact that establishing a succession plan works against every recommendation for good security practices. Security experts want you to create strong passwords, to use different ones for different accounts, and to change them frequently. How many times have you heard or read that you should never, ever write down passwords? Think about it. If you do a great job on security, you all but guarantee no one can get easy and timely access to your digital world when the time comes.

Here's another thought experiment: What if you use a thumbprint scanner or other biometric device for access to your computer? What happens when you die?

Similarly, it is not a great idea for security reasons to create directories, folders or documents on your computer that are named “Passwords,” “Important Financial Stuff” or “Account Information” in case someone breaks into your computer system or steals your computer.

Although you will occasionally read articles suggesting that you cover your digital assets explicitly in your will or trust or even create a unique document to cover them, the fact is that most of us do not get around to doing that. Our digital world and our digital assets change on a regular basis. Almost by definition, any document that we create will be out of date when the time comes to use it.

A Simple Five-Step Plan to Manage Your Digital Estate

While I doubt that any of us will be able to put together a foolproof and perfect plan for our digital assets and affairs, the fact is that most of leave our real-world assets and affairs in less than perfect order. However, we at least try to make things easier for our survivors who have to handle our real-world estate. The best we can do is to put things in order as well as we can, pick the right people to handle them, and leave reasonably clear instructions. I suggest that we want to try to do the same things for our digital estates.

Toward that end, I want to recommend a simple five-step plan that you can start on today and then revisit from time to time. In most cases, these steps have real world analogies and I encourage you to think in those terms. Build on what you know.

Step 1. Inventory Your Digital Assets.

I spent a large part of my early legal career as an estate planning lawyer. In the case of either death or incapacity, the first important step is to track down and identify all of the assets, liabilities and other concerns that must be addressed. Once an inventory is created, you can move forward with marshalling and collecting assets, identifying outstanding liabilities and paying them in a timely fashion, and dealing with outstanding issues, such as turning off utilities, canceling credit cards, arranging for storage or disposal and the like.

In the real world, your family and designated successors (personal representative of your estate, trustee of your trust or attorney-in-fact under a durable power of attorney) will be aided immensely by any list of assets and liabilities that you can prepare for them and leave in a place that is easy for them to obtain.

In your digital world, you also want to help your successors by creating an inventory. The more detailed and accurate the better, of course, but even a small start can be of help. Here are some of the things I suggest that you inventory:

1. **Hardware.** Inventorying your hardware seems like an easier project that it actually will be. I suggest that you create a list of your hardware with a summary overview of what is on it. Creating the inventory is likely to be an eye-opener for you. You are likely to find that you have important information not only on the computer system you use everyday, but also on multiple other computers. Many of us have at least one laptop and one or more desktop computers. Many people keep copies of vital information on their work computers. Where do you back up information? You might have many USB flash drives, USB hard drives, backup CDs or DVDs. There might be important pictures still on digital cameras and even information on iPods or other devices.
2. **Software.** Do you use Quicken or another financial program? What income tax preparation programs do you use? Do you create spreadsheets or Word documents with important financial information? If you blog, is there a program that someone would need to use to post news to your blog?
3. **File structures.** Your inventory should sketch out the main folders and places where you keep personal, financial and client files and documents. For someone like me, I also have audio and

video of presentations and podcasts that I'd want someone to be able to locate and deal with. You might have important collections of family photos or videos or work in progress.

4. **Online presence.** Create a list of your Web site(s), blog(s), Facebook and other social media accounts, online backup sites, online sites where you store documents, photos or other files, and listservs, groups or other sites to which you belong.
5. **Online accounts.** Amazon and other shopping sites make it easy for you to create accounts and include credit card information. You might also have online access to bank and investment accounts. In fact, in many cases, you might no longer be receiving paper statements for accounts. If you don't identify these accounts, it will be difficult for your successors to even know that they exist because there simply will be no paper trail. Also, make a list of all the e-mail accounts you have and use. Many of us have several e-mail accounts these days.
6. **Work information.** Lawyers might have access to client sites, collaboration sites, online document repositories or other information that no one else knows about. In addition, they might have access to software, online tools or online databases that someone taking over their work will need to have. In some firms, lawyers might have important network passwords, backup media or other digital assets the existence or value of which is not realized until they are gone.

At this point, you really want to gather and collect as much information as you can for your inventory. You can work on organizing and prioritizing later.

Step 2. Identify Appropriate Help.

In our estate plans, we typically name a surviving spouse or adult child, especially one with financial savvy, as a personal representative or trustee. That person, however, might well be the worst possible choice for dealing with our digital assets, especially if they are not computer savvy. We also recommend appropriate lawyers, accountants and financial planners to assist our survivors with our financial affairs after our deaths.

You will want to give serious thought to who should be looking into your digital assets on your demise and give thought to naming them in an official capacity in some cases or clearly identifying individuals as "go to" people in other cases. Here's a simple exercise to help you: Imagine that you have died or are incapacitated. Who do you want to turn on your computer to find out and deal with what's there? Let them know that and let others know that. If the IT person in your office could assist your surviving spouse, then make it clear that he or she should be engaged to help. A child you might not want making financial decisions might be just the one you want going through your digital world.

I also suggest talking to your estate planning lawyer to see if dealing with your computers and digital assets is something about which he or she has expertise.

Step 3. Provide for Access.

While we are all cautioned never to write down passwords and PIN numbers, the simple fact is that, if we do not do it and keep them in a safe place where they can be found at an appropriate time, no one

will be able to access our computers and accounts. This not only can cause delay, frustration and inconvenience, it can also mean that our best friends scattered around the country and world might well find out about our demise weeks after a funeral that they would have wanted to attend.

Unfortunately, as I mentioned earlier, good security means that your passwords are a moving target because you should be changing them on a regular basis. I still think it's useful to keep a list of passwords in a safe deposit box or other safe place that someone knows about. My old law firm routinely keeps important personal documents of its clients in a vault. Keeping a document with your passwords and other online account information with the other important documents will help your survivors. Another approach might be to tell your lawyer where the password list is kept and let him or her tell your survivors at the appropriate time so that it can be located.

Do not underestimate the difficulties that can arise from passwords. It is possible that some of us now have hundreds of passworded accounts. In most cases, you should be able to eventually get access to accounts with a death certificate and appropriate documentation. That should provide an alternative to the morbid ideas you might have had when I mentioned the thumbprint scanner issue earlier in this article.

Step 4. Provide Instructions.

I started with the story of Andy Olmsted because it is a perfect example of someone who knew what he wanted to happen and gave instructions for that to happen. Most of us will not reach a point where we will sit down and provide detailed instructions unless we face what I used to call when I did estate planning a "focusing event" – both spouses flying on the same plane, going into combat, terminal illness or the like.

There are a number of areas where your survivors would appreciate instructions:

- **Notifications.** Many of us now have Facebook "friends," LinkedIn "connections," Twitter "followers" and others we communicate with on a regular basis. If we have a blog or Web site, we might have people who read our words or visit our sites on a regular basis. If we want those people notified, we need not only to make our wishes clear, but to provide access to the tools and give instructions so that can happen. Think about Andy Olmsted's example. He wrote the post, but he had to let someone know that it existed, how to access his blog, how to post it to his blog, and how someone should respond to the comments the post would receive. There are instances now of survivors who continue to update Facebook accounts and provide other information online after someone dies.
- **Continuing or closing sites.** In my case, I have a Web site that's been around for almost 15 years and a blog with seven years of posts. I'm not sure that I really want that to disappear. It would still be a valuable resource if I were gone. If you want a site to continue, you will want to give instructions as to how that might occur (e.g., preserve what's there or perhaps have someone take it over and continue it). Even for sites or accounts that you want closed, you might want to be sure that a copy is made and kept, and that pictures, audio or video are saved.

- **Realizing value.** Let's face it, none of us are likely to realize the post-death financial revenues of Graceland and the Elvis Presley estate. However, simply shutting down sites might cut off potential revenue streams from e-books or other revenue-producing items. In the case of popular blogs, photography sites or online videos, your estate might be able to realize income from licensing, creating a book or taking other steps to "monetize" content. In some cases, you might have already started some of those projects.
- **"Do Not Delete" items.** People now routinely digitize all kinds of important document, photos and videos. For example, you might have scanned historical family pictures or family videos, or have a folder with the novel or screenplay you've been working on. If you intend that they be passed on, make sure that they are identified and not lost when a hard drive is deleted.
- **"Bequeathed" information.** As mentioned previously, you might be keeping family, business or other information that should be made available to specific people or even donated to a university or other archive.

Step 5. Give Appropriate Authority.

For some of us, and this might become more the case as time goes on, it makes sense to designate specific knowledgeable people and provide them with the appropriate authority to manage our digital assets. It might make sense to designate co-attorneys-in-fact, co-executors or co-trustees, where one is specifically tasked with taking the responsibility for our digital assets and affairs. Finding estate planning lawyers who are experienced and knowledgeable in "digital estates" will be essential in certain cases.

In addition, you might look into ways that your online accounts might permit you to designate others to act on your behalf or get added to your accounts. Especially in the cases of people who are not married or in a state where domestic partnerships would help, finding ways to give exactly the people the authority you want to manage your digital affairs will be very important. I expect to see this area continuing to evolve, with many areas of uncertainty.

Tips for Providing Assistance After the Death of Another

It's also possible that either as a survivor or as a lawyer, you might find yourself in a position where you need to handle someone's digital affairs. I have a few tips.

- Find knowledgeable technical and legal help.
- In the case of a death, try to get to contact lists, e-mail accounts and social media accounts to notify friends who the deceased would want to be notified.
- Change all passwords as soon as possible.

- Try to understand the totality of the person's online presence and identify some of the people he or she has interacted with most for assistance, especially in the social media platforms.
- Do not start closing accounts, shutting down hosting and e-mail, or taking other drastic steps until you have a good sense of the individual's presence and what you are ultimately going to do with it. Keeping a Web site up for a year or more will not be expensive. Shutting it down too early and losing valuable data could be quite expensive.
- Be slow to delete, but when you delete or dispose of computers and drives, delete in accordance with forensic standards so data cannot be retrieved by others.
- Spend \$100 on an external USB hard drive and make a copy of all hard drives, flash drives and other data and keep them in one safe place. Once you start to go through the data, you can keep another drive with the "good stuff."
- Make copies of Web sites and other online accounts.
- Locate all the financial information and client records as soon as possible and aggregate and isolate them.
- Remove credit card information from shopping accounts.
- Err on the side of keeping e-mail, documents and photographs for family members.

Start Thinking About Your Digital Estate Plan Today

The issue of what death means in the digital world has been with us for many years. It really started to come to public attention with the Iraq war, though, especially in terms of access/ownership of e-mail accounts and getting to online banking and other accounts by survivors of soldiers killed in action. Today, our lifetime digital presence has grown exponentially and the issues involved in handling our digital assets and affairs have also grown dramatically. If you take time to work on the five-step plan suggested in this article, ideally in connection with updating your estate plan, you'll help make things easier for your survivors and improve the chances that your wishes are followed. Read Olmsted's blog post, dry your eyes, and start on your plan today.

About the Author

Dennis Kennedy is an information technology lawyer and legal technology writer based in St. Louis, Missouri. He writes the monthly technology column for the *ABA Journal* and is a co-host of the legal technology podcast The Kennedy-Mighell Report, on the Legal Talk Network. His blog, DennisKennedy.Blog, is located at www.denniskennedy.com/blog.
