MEGAN YIP
LAW OFFICE

YOUR DIGITAL ESTATE

A Consumer Guide to Digital Asset Estate Planning & the Post Death Administration of Digital Assets

Funded By: Borchard Foundation on Law & Aging | Content By: Megan Yip & Willow Brugh

TABLE OF CONTENTS

DIGITAL ASSET ESTATE PLANNING

Estate planning, at its most basic, is making plans for what will happen to all the things you own and use at the time of your death. Some estate plans are aspirational: an annotated list or letter left for family and friends. Other estate plans are written to compel people to do what the plan says: a very detailed and persuasive letter, or documents that you give to a group of people who will hold each other accountable to fulfill your wishes at the time of your death.

The final kind of estate planning binds your loved ones and colleagues to comply with your wishes to use your assets in a certain way, or complete certain transactions, under law. This is primarily done through wills and trusts. The people who do this type of planning are often making plans for their children, may own real estate which has transfer requirements, or need to provide specific instruction for complicated assets. They often hire a lawyer to help them plan and execute legal documents which will direct what should happen when they die. Their lawyer will help them choose which documents to use to direct their assets and how to write those documents in order for their wishes to be legally binding.

Digital Asset Estate Planning is making and communicating plans about what should happen to your **digital** assets when you die. Defining and understanding digital assets is an important first step to Digital Asset Estate Planning.

We define digital assets as: files, photos, content, resources, or accounts that you have created, purchased, or primarily store in a digital format. Some digital assets you OWN, others you LICENSE to use. Those digital assets you own, you can pass on to others. The accounts you hold a license to access are unlikely to be transferable.

FAQ: ANSWERED

WHAT'S SO UNIQUE ABOUT DIGITAL ASSETS?

The term "digital asset" is an oxymoron. The "digital" in digital asset defines the form of the asset as an electronic record, which is by definition easily duplicable. An "asset" is usually defined as something of value. Quite often assets gain their value from their uniqueness. So when we talk about digital assets, we are talking about an easily duplicable (perhaps unique) thing of value.

These assets are considered "digital" because they exist because of technology. So to understand digital assets, we also need to clarify "technology."

Technology is a technique or device that solves a problem. Most of the accounts we are discussing when we talk about Digital Asset Estate Planning are unique, scalable solutions to a problem many humans face.

As we rely on technology to solve our communication, organization, or automation problems, we start to rely on the companies whose job it is to solve these problems. Our reliance on these companies and the solutions they provide can create unintended consequences. Technology can solve one problem while creating another.

The easily duplicable and shareable nature of digital assets makes managing digital assets different from managing physical assets. However, that doesn't change the fact that the management of any asset requires thoughtfulness and intention.

Given the rapid pace of technological change, lack of intentional management leaves digital assets both more difficult to keep private and also easier to lose at the point of death.

STEP 1: INVENTORY

> The first building block of digital asset estate planning is knowing what you have; so the first thing to do is take an inventory of the online accounts, software, and applications you use. If you use a password manager, you have a head start in creating your Digital Asset Inventory.

- **Make a list of all your digital assets.** Each day for a month, ensure the accounts you are using are on your list. Include all accounts, remembering:
    - Your email accounts (many people have more than one)
    - Your social media accounts
    - Your online file storage accounts
    - Your online gaming/hobby/social activity accounts
    - Your blog(s)
    - Your websites, including domain and hosting
    - Your online store accounts

Note

You can export an inventory list from your password manager. Our suggestion is to print it or export it to a spreadsheet without the passwords.

- **Subdivide your inventory based on use.** Once you have an inventory, it is a best practice to subdivide your inventory so you have a list for personal accounts and a list for work related accounts. Some people will find it useful to divide the inventory further by project or collaborator.

TAKE NOTE:
PASSWORD MANAGERS

Many folks (maybe that's you!) keep passwords in written format, share passwords with a family member, or have the internet browser remember passwords. These are understandable ways of dealing with your accounts – remembering passwords is hard!

The area of study dedicated to thinking about how computers store and transmit information to authorized and unauthorized users is called Information Security, sometimes abbreviated to "InfoSec." InfoSec experts have long advocated for "strong" passwords, meaning they should be long, with many strange characters. For instance, "password" is not a good password; neither is "1234". A great password looks like this: 2=7Am8,KI5eOL!3AnvbGHjT. But how would anyone remember something like that to actually use it?!

Luckily, smart people created something called a Password Manager. A number of companies now provide password managers for an annual or monthly fee. They all basically work like this:

1. You create a vault, which requires one main password to lock and unlock.
2. The program helps you create and then store those strong passwords in the vault.
3. By unlocking that vault, always with that same main password, you can use all the other passwords you need to have access to. You don't even have to remember which password goes to which account – the vault does that for you!

This means that you need to remember one strong, memorable, password, like "t00muchlightmakesthebabyg0blind!". Then, because the program is remembering the rest of the passwords for you, those passwords can be long and complicated and unique for each site like: D7z8~t;adn4VfLqR!LhUzLlix-}sSH6H|1, which prevents others from guessing them. It's like carrying around a bag full of keys. You only have to remember the one bag in order to have all the keys with you.

Please take a look at some password managers – do a search for "password manager" and read what others have to say about them.

Digital Asset Inventory Example:

WORK ACCOUNTS			
Account/Software/Application	**Primary Use**	**Value**	**Death Plan**
Work Email *Smith@Company.com*	Everything		
Work Cloud Storage	Sharing data with clients		
Work File Storage	Backup client data		

PERSONAL ACCOUNTS			
Account/Software/Application	**Primary Use**	**Value**	**Death Plan**
Personal Email:	Ocasional		
SportsTeamFn@emailco.com	correspondence with friends		
Google drive	Family photos & videos		
Shutterfly	Family photos		

STEP 2: DEFINE VALUE

Make Notes about how you use this account. Describe your primary use for each account or asset in the next column.

Consider the following:

- Why did you open this account or start using this application?

- What is stored in this account? Who do you communicate with via this application?

- Is this something you keep online (in digital format) to keep it private, to share it with a select group of people, or to share it publicly?

Include Information about what value it holds for you and others.

- What is the value of this asset to you?

- Does anyone else access this account or what it holds? Does anyone rely on your use or access of this account?

- Do you use this account to communicate with certain people? Do they have other ways to contact you?

Example:

Account/Software/Application	Primary Use	Value	Death Plan
Work Email *Smith@Company.com*	Everything	High $ and practical value to employer and colleagues	
Google drive	Family photos & videos	Sentimental/ historical family history	
Shutterfly	Family photos	Sentimental	

STEP 3: PLAN FOR DEATH

Make a Note about What Should Happen at the Time of Your Death: Review your inventory, while giving consideration to the use scenarios, and valuation notes. Ask yourself what should happen to each item on your inventory at the time of your death.

Account/Software/Application	Primary Use	Value	Death Plan
Shutterfly	Family photos	Sentimental	Goes to eldest offspring
Work Email *Smith@Company.com*	Everything	High $ value to employer and colleagues	Goes to manager
Google drive	Family photos & videos	sentimental/ historical family history	Goes to youngest offspring

STEP 4: HOW TO MAKE YOUR PLAN LEGALLY OR TECHNICALLY BINDING

Consider the following strategies to make your plans binding. Some mechanisms are legal, but we also believe tech strategies or tools are an important part of Digital Asset Estate Planning.

CONSIDER THE LAW

Keep in mind that the law is still developing in the digital asset estate planning space and as a result there is a lot of uncertainty. A number of laws each speak to a certain aspect of the concerns presented by the management of digital assets at the time of death, but there is no law that addresses all of the concerns in a clarifying manner.

Most states have adopted a uniform law called the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) that provides a framework for digital assets to be transferred to executors and family members with a judicial order from a probate court. However, Federal Privacy law and the Terms of Service of many internet companies do not provide for the transfer of certain digital assets.

Technology companies may incur liability under the Electronic Communications Privacy Act (ECPA) if they release private communications to anyone other than the original account holder.

Intellectual Property laws create and protect our ownership rights in the things we create. We do a lot of creating and sharing of things we create on the internet. Thanks to Intellectual Property laws, we have ownership rights in the photos we take and the blog posts we write online, even when they're hosted on a company's website.

A Terms of Service contract is what governs the relationship, we, the users, have with the internet companies who provide services and solutions to us. The important thing to know about these contracts are that the majority of internet companies are contracting with us based on a non-transferable license to access their website and the computers that run or host their web-site and the services it provides.

So, we might own and have a right to transfer what we created and store or share in an internet account thanks to intellectual property laws, but because of how the terms of service of an internet company work, we cannot transfer the rights to access the account we used to create or store the intellectual property.

Sharing passwords also presents legal concerns. Most Terms of Service prohibit both sharing passwords and accessing accounts that you did not create. It's true that many people rely on the fact that these specific terms of service are rarely enforced. However, during a negotiation to access or receive content from a deceased person's account, a company is very likely to track if anyone has accessed the account in question since the time of death and also take note of Terms of Service violations.

The Computer Fraud and Abuse Act (CFAA) is one of many anti-hacking laws meant to make it illegal to access computers that do not belong to you. The CFAA has both civil and criminal penalties. It's important to be aware of whose computer you are logging into when you access an account. You may have permission from your deceased family member to access their account.

However, in most cases you do not have the internet company or service provider's permission to access their computers. Keep in mind, when you log onto a service provider's website with a family member's credentials, you are accessing the service provider's computer without their permission. The CFAA presents a notably unsettled corner of the law. The consequences of running afoul of the CFAA can be surprisingly severe, including jail time.

Even though the realm of digital assets is unsettled, there are still some strategies to make your plans binding.

CONSIDER IN-APPLICATION TOOLS

The first thing to know is that some of the larger websites (at the time of this writing, Facebook and Google) have designations on their website within your account where you can say if anyone should have access to a part of your account when you die. You can select and confirm within your account for the transfer of assets as allowed, or designate that account deletion should occur when the company receives notice of your death. The same way a beneficiary designation on a financial account supersedes a directive in a will or trust, the in-application designation on a website will supersede what is written in a will or trust.

PRIORITIZE & DRAFT FOR WHAT'S MOST IMPORTANT

The next best practice is to prioritize your most important accounts and draft those into your legal estate planning documents. If your financial livelihood or the majority of your family's photographic memories are connected to one account or platform, then prioritize creating a legal or technical plan for that account. Specific accounts, if it is allowed by the company's terms of service, may be transferred on death. Confirm this by reviewing the company's Terms of Service and other policies. The best way to ensure the transfer occurs is to specifically describe the account, what it is used for, and who should have access to it in the future in your estate planning documents.

CONSIDER TECHNOLOGY

Given the technical nature of digital assets, keep in mind that the best way to ensure that your data, photos, or information are transferred to a loved one or deleted on your death may be to change where those digital assets are stored. Backing up, switching storage providers, or printing out on paper, are important strategies that should be considered when deciding how to make your digital asset estate plan fool-proof. It is a best practice to include an IT professional or a very tech savvy family member on your team when you are planning to fool-proof your digital estate plan.

- **Review the Terms of Service and policies of applications you use.** Is the account transferable on death?

- **Review how the accounts and applications you use regularly function.** Can you share access to an account, files, or application now?

- **Write down the steps you will take, or have already taken to make your plan binding.**

Use this final column of your spreadsheet as a To Do List for meeting with your Attorney and IT Professional.

Account/ Software/ Application	Primary Use	Value	Death Plan	Steps to Make It Binding
Shutterfly	Family photos	sentimental	Goes to eldest offspring	Back up photos onto hard drive, print out photo books for grandchildren
Work Email *Smith@Company.com*	Everything	High $ value to employer and colleagues	Goes to manager	Covered under employment contract - leave note on list for executor to notify boss and not use
Google drive	Family photos & videos	sentimental/ historical family history	Goes to oungest offspring	Activate Google Inactivity Manager in Google account settings with _____named

FAQ: ANSWERED

WHAT ABOUT THAT BROAD SWEEPING LANGUAGE IN MY TRUST?

Many attorneys are drafting clauses into estate planning documents that give an executor or trustee permission to access all of a deceased person's digital assets. This may provide proof of intent and shield the personal representative from some liability. However, if this language is encountered after death, there will still be quite a lot of work to be done.

For example: if the Trust of John Doe is presented to an online service provider, how will they know the Trust of John Doe and the death certificate of Jonathan D. Doe actually correspond to the platform user @gameshowguy? After confirming whether the digital asset is transferable at all, the estate administrator will have to prove to the service provider that the digital asset corresponds with the description of digital assets in the document and that the account owner is represented by the death certificate that is presented.

FAQ: ANSWERED

HOW TO CONSIDER APPS AND SOFTWARE PROMISING A DIGITAL ESTATE PLAN SOLUTION?

Although digital asset estate planning isn't as popular as social media or online gaming, there are still technology solutions popping up in the space. How should we consider the technology solutions and apps that are promising to help solve our digital asset estate planning needs?

Like any technology solutions, make sure the technology is addressing a problem you have. Make a list of the problems you are trying to solve; evaluate the software against your priorities and concerns; investigate what the company is doing with the data they are storing for you.

- Are they accessing or using it in other ways?
- Is it encrypted?

Make sure they are not over promising something they cannot provide. Ask technically savvy people in your life or look at Consumer Reports to get a feel for what is technically feasible if you aren't sure yourself. Consider their business model.

- How do they make money?
- Is the company likely to be around longer than you are?

It's relatively easy and mostly an act of self discipline to organize and document what you own and use regularly and why. It is quite a bit more difficult, and sometimes practically impossible, to legally insure your wishes are completed, especially when it comes to digital assets. Remember advice given by lawyers and documents created by lawyers are protected by malpractice insurance in most cases. Technology companies and their solutions are not required to insure their work or the promises they make in any way.

POST DEATH ADMINISTRATION OF DIGITAL ASSETS

Post Death Administration is the work of transferring assets of the deceased, closing accounts, and passing on things that the deceased person used. Post Death Administration is when we find out how good the estate plan really was. Dead people can't own or take care of things and so others administer the assets of the deceased. If the estate plan is not thorough or if the language is unclear, post death administration is more difficult. All assets go through some sort of post death administration. Bank accounts are claimed by family members of the deceased or are transferred to the state if they are unclaimed. Personal property of the deceased is moved out of apartments by loved ones or their landlord. Let's look at how the post death administration of digital assets goes.

1. LEARN WHAT YOUR ROLE IS & WHO OWNS THE ASSET:

- **Are you the named executor or personal representative of the estate?**

One of the most important jobs of a will or trust document is to name the person who will be responsible for administering your estate after you pass away. Some folks are now naming "digital executors" as well. Others are specifically delegating the authority to act on one's behalf with regard to their digital assets to the person named in their will or trust.

If you have been named a digital executor or been given the authority as a personal representative or trustee to take care of someone's digital assets, that is the best case scenario. If the estate planning documents do not clearly name someone to be in charge of digital assets, there is a logical assumption that the fiduciary duty they have to control the assets of the estate in the best interest of the beneficiaries extends to digital assets. However, it's important to understand that being the named executor, personal representative, or closest family member of the decedent does not necessarily entitle you to access all digital assets. If you are a personal representative or trustee, the right thing to do may be to manage the potential value or liability presented by the digital assets with as little access to them as possible.

- **It is not always obvious who owns a digital asset.**

Most people access accounts or use software that is owned by their employer or co-owned with a business partner or other colleagues. Great care and consideration should be given to digital assets that might include private information or information owned by an organization or entity that the decedent was a part of, but that you as a family member or executor are not a part of. In these cases, the software owner's wishes are more important than the decedent's wishes or your wishes. Communicate with employers, business partners, and artistic co-collaborators before accessing or taking action on digital assets that might belong to someone beside the deceased person. Many digital assets are not owned by a person and so the permission to access them terminates at death. Not all digital assets are transferable.

2. SORT OUT WHAT THE DECEASED PERSON'S WISHES WERE

In the best case scenario, you will find a complete digital asset inventory including notation about what the deceased person wants done with each of their digital assets in case of death. Furthermore, we hope that others who might be involved understand the same wishes. Finally, it would be great if the technology is set up in a way that matches what is described in the documents you've found. If the digital asset inventory is part of a larger estate plan, you should read all the legal documents that are part of the estate plan. Sometimes reasoning across the documents is interconnected, and it should be considered as a whole rather than piecemeal. If you find the documents confusing or intimidating, make an appointment with an attorney so they can help you interpret the documents to sort out the decedent's intentions or hopes in leaving the estate plan in this order. If you find the inventory and do not know where the rest of the estate plan is, it is important to speak with others who may know where the decedent might have kept important documents including their estate plan.

3. DELETE OR TRANSFER ACCOUNTS

The purpose of an asset inventory (digital or otherwise) is to use it as the basis of a plan to systematically transfer and distribute assets in accordance with someone's estate plan or the Probate Code's default scheme which we refer to as intestate succession.

DELETE ACCOUNTS

One thing unique to digital assets is the ease of closing or erasing online accounts. Consider that many people actually want a substantial amount of what they do on the internet kept private and so would prefer to have their accounts deleted. If someone has requested or made an annotation to delete the account, you should do that. The best practice would be to delete it by contacting the company or platform and reporting the account user as deceased.

Here are some other reasons to Delete Accounts:

- If there is a risk of someone using the online profile or information on that account to commit fraud by impersonating the deceased with intent to harm or take advantage of others, then you should delete that account.
- If the account represents a pay-to-use service and there is nothing in the account of value to the estate, then the account should be deleted to avoid waste of the monetary assets paying for the service.

TRANSFER ACCOUNTS

If the account is transferable, then work with the company to follow the decedent's wishes to transfer the account.

4. CONSULT WITH PROFESSIONALS

Attorneys and IT Professionals can provide the most help if you have any questions about what you should do related to a deceased person's digital assets.

If you are unsure of your role or have questions about estate planning documents you've found, contact a probate or trusts and estates lawyer.

If you don't understand who owns an online account or the information in an account, or if you are confused about whether an account is transferable an attorney should be able to help. They should consult local law, case law, and the Terms of Service of the product or service to determine ownership and transferability. Remember to also ask questions about the potential liabilities related to accessing the account of a deceased person without permission, or deleting an account before you understand its primary use or value.

If you have questions about how someone else's technology is set up and why, ask an Information Technology Professional. If you have a basic question about how something works or where to find certain information, asking anyone you know in the information technology sector is a wise move.

If you are trying to access data that is intentionally protected or encrypted or trying to determine what someone else's technology does and why, its advisable to work with an attorney and an IT Professional who can advise and assist you in carrying out the deceased person's wishes while also respecting the ownership interests and privacy of others.

WORST CASE SCENARIO: NO INVENTORY FOUND

What if a friend or other loved one has passed away and there is no digital asset inventory found? This can feel scary, but just because the list does not exist does not mean the items that would have been on the list are not discoverable.

BUILD A LIST

Remember the information is out there, even if it's not compiled for you. Review the previous section about Making an Inventory and think about how you might build the same list for another person. You already know about some accounts based on your online interactions with them – maybe their Facebook, Twitter, or email account. Check for a paper trail – did they print out receipts for paid online accounts? What accounts did they need at work, or did they use to connect with coworkers? Put together a list of accounts that you discover or expect they might have.

FIND MORE LOOSE ENDS

To reach beyond what you (and others) know, consider running an internet search for the decedent's name or handle (online nickname). Do these seem like they were also theirs? There are a few services which can help you locate assets online. You might look at tax returns.

ESTIMATE WISHES

Now that you have a list, consider what the person's wishes about each digital asset might have been. Talk with friends and family connected to the account for a gut check. If you don't find things, take heart and remember that many people use websites for activities they see as ephemeral or that they want to remain private or anonymous.

TAKE NOTE:
BEWARE THE TEMPTATION OF PASSWORDS

Your deceased loved one may have left a list of passwords with their accounts, or you might come upon a list of passwords in sorting through their important papers and notes. You may be tempted to log-in using their passwords post death, but beware of the risks involved with this temptation. Unless there are documents specifically directing you to access their accounts by password or giving you permission to access their accounts with their passwords to do specific work, you shouldn't log in with their account. Even if you have these documents, sharing passwords is often a Terms of Service violation, which can make further interaction with that account complicated. For instance "I know this bill got paid last week online but my partner has been dead for two weeks" is a difficult conversation to have. Act in alignment with the Terms of Service to have a clearer path to resolution.

TAKE NOTE:
DON'T IMPERSONATE OR FRAUDULENTLY USE ASSETS

You make think it's clever, or a good way to keep a memory alive to impersonate the deceased, especially through social media. The temptation to keep someone's presence alive or to use their accounts in their shoes for ease of transactions is substantial. However, this kind of confusion is illegal and violates both public policy and specific site policies. Furthermore, this type of thoughtless impersonation can invite bad actors who want to harness the confusion to misuse the assets which haven't been transferred yet or take advantage of grieving family members.

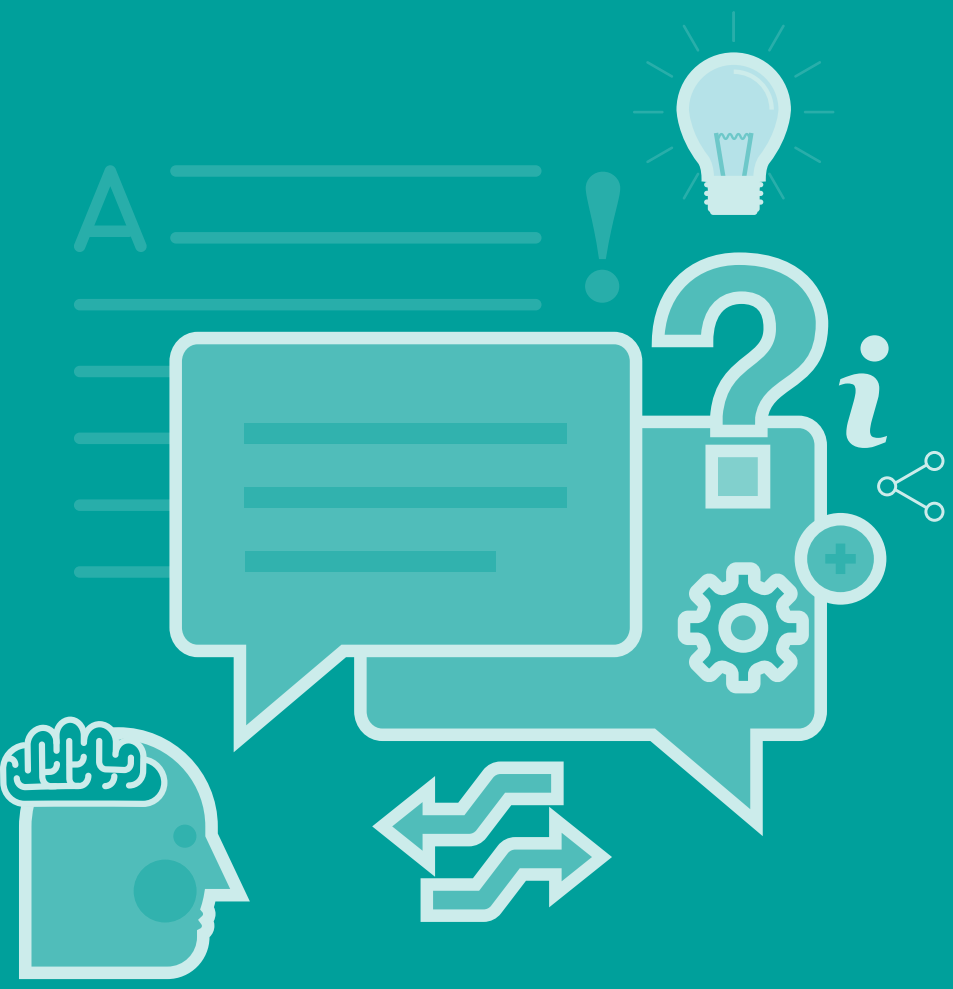
Consider other online memorials or established memorialization techniques to keep your loved one's memory alive in your internet community.

FAQ: ANSWERED

WHAT IS A "GOOD" QUESTION?

"Good" questions to talk about as an executor with the person who has asked you to be their executor might include the following:

- Do you have an inventory of your assets including digital assets?
- Where do you store that inventory, and how would I gain access to it?
- What sorts of accounts do you have, and how do you want them to be used after your death?
- What accounts should be deleted?
- Do you co-own accounts or digital assets with anyone?



IN CLOSING: HAVE A CONVERSATION

Talking about death is difficult. You have to be vulnerable. And it's the only way to make death easier. If you have the conversations now, there will be less stress at a time of incapacity or death.

Talk to your friends and family members, especially those who you have named to be your trustee or personal representative, about what you would like them to do with your digital assets or online accounts.

If you know that anyone is naming you as a trustee or personal representative in case of incapacity or death, ask good questions before the worse case scenario occurs. Remember to ask them about their digital assets and online accounts, not just their traditional assets (home, car, and bank accounts).

GLOSSARY

App/Application: App is an abbreviated form of the word "application." An application is a software program that's designed to perform a specific function directly for the user or, in some cases, for another application program.

Beneficiary: A person who derives advantage from something, especially a trust, will or life insurance policy

Computer Fraud and Abuse Act (CFAA): A United States cybersecurity bill that was enacted in 1984 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984.

Decedent: A person who has died.

Digital Asset: We define digital assets as: content, files, resources, or accounts that you have created, purchased, or primarily stored in a digital format. Some Digital Assets you OWN, some you LICENSE (access/accounts/software). Digital assets you own you can bequeath or pass on to others. Those you license are unlikely to be transferable. Many people are still sorting out their definition of digital assets. Different laws include definitions of digital assets.

Electronic Communications Privacy Act (ECPA): The Electronic Communications Privacy Act of 1986 (ECPA) was enacted by the United States Congress to extend restrictions on government wire taps of telephone calls to include transmissions of electronic data by computer (18 U.S.C. § 2510 et seq.)

Estate: All the money and property owned by a particular person, especially at death.

Executor: A person or institution appointed by a testator to carry out the terms of their will.

Fiduciary: (Relationship or Role) Involving trust, especially with regard to the relationship between a trustee and a beneficiary

Intestate Succession: Refers to the law of the State providing for the inheritance of property from a person who dies without leaving a will. Thus, to carry out a "intestate succession" simply means to transfer something after the owner has died and in accordance with the State law of intestate succession.

Intellectual Property: A work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.

IT Professional: IT stands for Information Technology. An IT Professional refers to someone who works professionally in the Information Technology sector.

Personal Representative: A personal representative or legal personal representative is a person appointed by a court to administer the estate of another person.

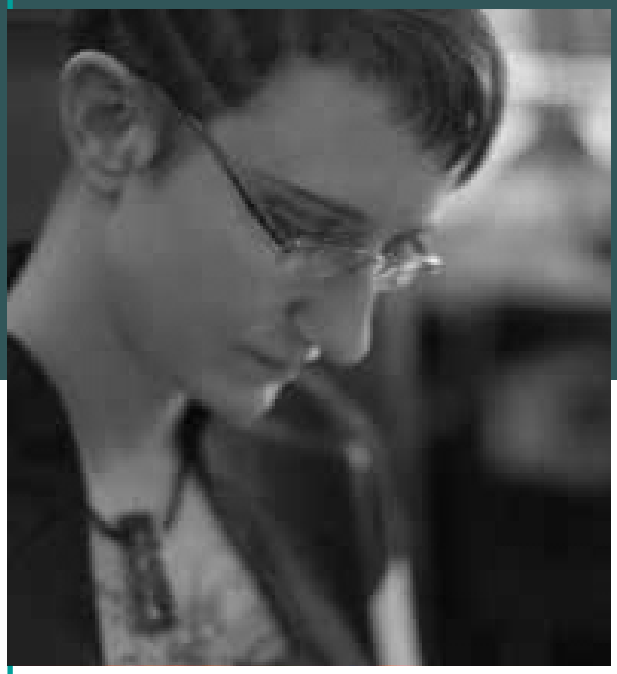
Private Communications: Private Communications is a term with a specific legal meaning under the Electronic Communications Privacy Act.

Probate Code (Probate Law): Probate is the process of proving a will is valid and thereafter administering the estate of a dead person according to the terms of the will. It is a judicial act or determination of a court having competent jurisdiction establishing the validity of a will.

Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA): A law developed primarily by the Uniform Law Commission (ULC) to provide fiduciaries (like executors and trustees) with a legal path to managing the digital assets of deceased or incapacitated people

Terms of Service Contract: Terms of service are rules by which one must agree to abide by in order to use an online service.

Trustee: A person given control or powers of administration of property in trust with a legal obligation to administer it solely for the purposes specified.



WILLOW BRUGH

Willow Brugh, known as willowbl00, works with digital tools to enable coordination between groups of all sizes and shapes. They have studied citizen engagement and combining distributed and centralized decision making structures at the Center for Civic Media at MIT's Media Lab, been a Professor of Practice at Brown University, an affiliate at the New England Complex Systems Institute, and a fellow at Harvard Law's Berkman Center for Internet and Society. They currently do operations and internal people systems at govtech consultancy Truss.

In brief, Willow looks at connections, systems, empowerment, and powerlessness and strives to both understand and improve whatever they find. Sometimes that's with the Occupy Sandy Movement, sometimes it's with the National Defense University. They have keynoted the IEEE Global Humanitarian Technology Conference. Willow has successfully worked with FEMA Field Innovation Team for Hurricane Sandy, and was awarded at a ceremony at the White House for their contribution.

MEGAN YIP

In her practice as an Estate Planning Attorney, Megan Yip helps attorneys, technology companies, individuals, and organizations address how to better plan for difficult situations presented by incapacity and death, in a world with an ever-changing tech landscape. She provides information, tools and resources to guide people through the maze of what should be done with digital assets in the case of incapacity or death.

Megan started her legal practice in California as a Fellow with the Borchard Foundation Center on Law & Aging with a placement at Legal Aid of Marin, where she focused on expanding services provided to low-income older adults in Marin County, focusing on consumer, housing and end-of-life planning issues. From 2011 to 2014, Megan worked at Twitter, Inc. on the Trust & Safety team focusing on site rules and policies addressing sensitive issues, including impersonation, online abuse and deceased users.

We give a special thanks to the Albert & Elaine Borchard Foundation Center on Law & Aging for providing us with a former fellow grant to work on this consumer guide.

The purpose of the Former Fellow Grant program is to award grants to support former Borchard Foundation Center on Law & Aging fellows in their continuing work in law and aging. More information can be found at: www.borchardcla.org/