# Start-ups – Legal Matters

## A. First Things First!

In my experience, the last thing an entrepreneur wants to think about is dealing with lawyers. As a fellow entrepreneur, I understand that the primary focus is developing and advancing your business. It is essential to have the right administrative framework in place to accomplish this. Taking care of the "legal stuff" is a necessary part of that framework. This article touches on some fundamental legal questions for a start-up:

- Which form of business organization is right for you?
- How do you identify and protect your brands?
- What steps are necessary in developing and maintaining your proprietary information?

### 1. Businesses come in many forms

One of the very first decisions an entrepreneur needs to tackle is which form of business organization is the right one. There are many options, ranging from a sole proprietorship, where the legal identity of the business and the individual are the same, to a limited liability company, or LLC, that can offer many flexible options in terms of structure ownership, yet being a distinct legal entity for liability purposes. The industry you are entering may itself be an important factor in deciding your business form – a web designer's structure may be very different than what is required to open a hair salon.

The right organization form depends on several other factors, including:

- The cost of formation, which will vary depending on the type of business organization (as well as the potential cost of dissolving the business, depending on which form you choose)
- Who may control the organization, whether it is a single individual or group of people or entities
- Whether the organization, like a traditional (or "C") corporation will be responsible to pay taxes or whether any tax liability will flow through to the owners, like in a partnership
- The potential liability for things that can go wrong in the business – a sole proprietor can face personal liability while the sole shareholder of a corporation, under normal circumstances, would not.

Should you choose to incorporate, another important decision is the state of incorporation. Many businesses incorporate in the state in which they are located. Others choose Delaware or other states whose laws are considered to be "business-friendly." Realize that the choice you make can increase the cost of setting up your business, as each state sets its own fees for incorporation.

The best thing an entrepreneur can do before making this decision is to consult with a corporate lawyer (*not me, but I have friends who are great corporate lawyers!*) who will help you determine the right structure for your particular business.

## 2. Brand identification and protection

In conjunction with deciding on your business structure, you need to settle on a name, catch phrase or logo for your business as well as any products that you are launching. Because your brand is a source identified, using your own name (*like Ossian Law P.C.*) is generally a safe bet. If you are choosing a different name, you want to make sure that the name is not already in use by a competitor or potential competitor or the subject of an existing federal trademark registration. Try to avoid a name that is description of the product or services you are offering. For example, "Mush Inc." would be a better choice than "Alaska Dog Sleds" for a dog sled company in Alaska.

You don't want to find yourself on the receiving end of a cease and desist letter because the name you picked violates someone else's mark. Establishing a brand is difficult enough without having to abandon and re-establish a new one. Some steps to avoid this situation include:

- An Internet search of the name to see what existing uses comes up. This may be a good first step, but should not be the end of your due diligence
- A search of the Trademark Database on the U.S. Patent & Trademark Office website: http://www.uspto.gov/trademarks-application-process/search-trademark-database
- A more thorough search by a trademark attorney (*again, not me, but I have friends with lots of expertise)* who can counsel you further on name choices
- Deciding whether and when to federally register your marks and in what classifications. You can do this yourself online*, (as I did with my catchphrase "Keeping IT Legal"® but even I had guidance from a trademark attorney friend*) or use the services of a trademark attorney which, in my opinion, is well worth the cost

Obtaining a federally registered trademark isn't where the work ends; you are required to police your mark, as discussed in more detail, below.

## 3. Developing and protecting your business secrets

Another important legal topic is the protection of the materials and information that are proprietary to your business. For a software company, this could include any applications, source code and documentation. For a restaurant, it could include recipes, suppliers and pricing. Regardless of industry, a fundamental matter is to make sure you either own or have sufficient rights in the materials

and information that is proprietary to your business. It is also key to protect that proprietary information when dealing with others. Some steps to take in this area include:

- Making sure that proprietary content is either created by employees or others with whom you have proper contractual agreements. If your business is relying on contractors or other companies to create proprietary information, you may need to get an assignment of copyright interests that might not otherwise vest in your business
- Requiring potential investors, business partners and others with whom you may be sharing proprietary information to sign appropriate non-disclosure agreements
- Having employee non-disclosure agreements, policies and procedures
- Employing other technical and administrative measures designed to protect proprietary information

Again, this is a subject area where consulting with an attorney (*finally, an area that is within my wheelhouse!*) to determine the right contracts and policies to put into place.

Starting a business is an exciting endeavor, but overlooking the fundamental legal steps could derail your business from its path to success.

## B. Protecting Your Public Face

This next section includes discussion of important steps to protect your business' "public face" from a legal perspective. Specific topic include:

- The importance of customer agreements
- Having contract terms that "fit"
- Enforceability of click-through agreements
- Privacy policy or other legal notices

### 1. Avoiding "he said/she said"

There are many benefits to having a written agreement in place between you and your customers. For one thing, both you and the customer have a writing to reference back to regarding the key business terms, such as price, quantity and service scope as well as legal protections like choice of law, jurisdiction, warranties, indemnification and limitations on liability and damages.

A written agreement also survives the departure of personnel that may invariably occur on either side over the course of time. While a verbal agreement in most instances may be legally enforceable, it is generally easier to prove and, therefore

enforce, a written agreement in the event of a party's breach. Not having a written agreement with your customers may lead to unnecessary uncertainty and disputes.

## 2. Where to start

Having (hopefully) convinced you that, regardless of the nature of your business, a written customer agreement is a must, the next question I'll discuss is "what terms do I need to include in the agreement?"

As an Information Technology transactional attorney, I counsel, draft and negotiate technology-related agreements on behalf of my clients on a daily basis. As an entrepreneur starting my own law practice over five years ago, I also had to think about what terms would govern the services my firm would be providing to my clients. My goal was to craft a concise engagement letter that contained the relevant terms of the engagement, including:

- Scope of the project(s) involved
- Fee structure and payment terms
- Methods of communication between my firm and the client
- How the engagement could be terminated

I began by looking at model engagement letters offered by the bar associations to which I belong, the American Bar Association[1] and the State Bar of Michigan[2]. Based on the model letters I reviewed, I was able to use some of the language in the engagement letter that I ultimately utilize for my firm. There were also clauses that didn't apply to my type of practice, so I didn't adopt those.
It is important for me to have a written agreement in place with each of my firm's clients that accurately reflects the terms of the specific engagement, not only because it is a good business practice but also because legal malpractice carriers strongly recommend that lawyers do so[3].

Where can you get ideas for your own customer agreements? Just as I did, you can start with any industry groups that may offer sample agreements[4]. Odds are

---

[1] http://www.americanbar.org

[2] https://www.michbar.org

[3] CNA Professional Counsel, *Better with a Letter: Why Attorneys Should Use Engagement Letters*, available at http://www.cnapro.com/pdf/CNA_LAW_ENGAGE_CNA_SEC.pdf

[4] A starting point could be a directory of industry associations. For example, job-hunt.org's Directory of Professional and Industry Associations and Societies is available at http://www.job-hunt.org/associations.shtml

that an off-the-shelf sample agreement is not going to be a perfect fit for your business and will need to be modified or enhanced in order to accurately reflect the particular deal. Depending on the nature of your business, you may have more than one type of customer or transaction and require several different standard agreements.

### 3. The right fit

Realize also that your agreement is a "living" document. I tailor my engagement letter for each client, changing or adding terms as needed. Some clients may even have their own standard professional services agreement that can be signed in place of my firm's engagement letter. The point is to make sure that the agreement you sign reflects the nature of the engagement or transaction that it is intended to cover.

If your business is operating online, for example, having a click-through agreement for customers makes sense. Online agreements and e-signatures, in most situations, are enforceable under federal[5] and most state law[6]. Be aware that some courts have not enforced certain terms of online "terms of use" where the customer was not required to scroll down and "agree" to the terms (sometimes referred to as a "browsewrap" agreement)[7].

Whether online or embodied in online terms of use, be sure to update your agreement to reflect changes in business or other key terms. Reviewing your standard agreements at least once a year is a good practice, but may not be sufficient depending on how rapidly your business is growing or changing. You

---

[5] The Electronics Signatures in Global and National Commerce Act, known less formally as the E-Sign Act, has been in place for almost 15 years and provides general recognition for the validity of electronic records and signatures. More information on the E-Sign Act is available at https://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf

[6] All but three states have enacted the Uniform Electronic Transactions Act. Only Illinois, New York and Washington have not done so, but each of these states have different laws addressing electronic transactions. For more information, go to: http://www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx

[7] See, for example, Nguyen v. Barnes & Noble Inc., Case No. 12-56628 (9th Cir., Aug., 2014) available at http://cdn.ca9.uscourts.gov/datastore/opinions/2014/08/18/12-56628.pdf

may want to avoid including a right to update your terms unilaterally, as some courts have held that this impacts the enforceability of the terms[8].

At the same time, a number of courts have held that terms exchanged between parties via email can form a binding contract[9]. But that is a topic for another day.

## 4. Privacy matters

In addition to a customer agreement (either hard copy or online), depending on the nature of your business and operations, you may also need a privacy policy or notice. Financial institutions are subject to the Gramm-Leach-Bliley Act, or GLBA, a federal law that requires a privacy policy and annual notice to customers and consumers[10]. Other federal laws, like the Health Information Portability And Accountability Act (HIPPA) mandate privacy policies and practices with respect to protected health information[11].

Even if you are not in a highly regulated industry like banking, insurance or health care, a privacy policy or notice may be appropriate. The Federal Trade Commission is a long time advocate for "privacy by design" including greater transparency over business' collection and use of consumer information[12].

If you are collecting sensitive information from clients, such as credit card numbers, social security numbers or other personally identifiable information, a privacy policy should effectively notify a customer of what information you are collecting, how you share it and related topics like how a customer can update the

---

[8] See, for example, Discount Drug Mart, Inc. v. Devos, Ltd d/b/a Guaranteed Returns, Case No. 1:12 CV 00386 (N.D. Ohio, Oct. 2013) available at http://www.gpo.gov/fdsys/pkg/USCOURTS-ohnd-1_12-cv-00386/pdf/USCOURTS-ohnd-1_12-cv-00386-0.pdf

[9] See, for example, Home Source Industries, LLC. v. Freightquote.com, Inc., Case No. 14-2001 (D. NJ, Nov. 2014) available at http://law.justia.com/cases/federal/district-courts/missouri/mowdce/4:2014cv01037/118865/27/

[10] More information on GLBA is available at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[11] More information on HIPAA is available at http://www.hhs.gov/ocr/privacy/

[12] FTC Commissioner Brill recently spoke on this topic at Carnegie Mellon University. The text of her speech is available at https://www.ftc.gov/public-statements/2015/01/its-getting-real-privacy-security-fairness-design-internet-things-keynote

information you have collected. As with customer agreements and online terms, make sure that the statements in your privacy policy or notice accurately reflect your current business practices (including those of any subcontractors with whom you are sharing customer information).

### 5. Other public-facing media

Finally, when considering customer agreements, terms of use and privacy policies, don't overlook your web site, blogs, social media pages and other places where your business is presenting itself to the public. While Facebook has its own lengthy terms of service[13], you may (and perhaps should) add your own additional terms on your business' Facebook page. An example is the University of Michigan Health System that includes its own "Social Media Terms and Conditions" under the "More" tab on its Facebook page[14].

To recap, written customer agreements are an important consideration for nearly every business, so:

- Look for industry-based resources don't forget to consult an attorney familiar with your industry and business practices to craft agreements that make sense for your business
- Tailor contract terms as necessary given the particular transaction
- Maximize the enforceability of your online terms by requiring a click-through and avoiding unilateral changes
- When adopting a privacy policy or notice, strive to make it transparent and reflective of your data collection and sharing practices
- Remember to include terms on social media pages, blogs and other web pages, as appropriate.

## C. Balancing Big Data and Privacy

This next section will discuss approaches to managing and utilizing the benefits of "Big Data" while remaining compliant with current and emerging privacy protection regulations. Specific topic include:

- Formulating a data strategy for your business
- Setting consistent data policies and procedures
- Aligning your business partners
- Maintaining transparency with customers

---

[13] https://www.facebook.com/legal/terms

[14] https://www.facebook.com/UniversityofMichiganHealthSystem/app_190322544333196?ref=page_internal

## 1. The Era of Big Data

In our ever-increasing connected world of cloud computing, smart devices and the Internet of Things, data is undoubtedly a major economic driver. The proliferation of data is mindboggling. It is estimated that 2.5 quintillion bytes of data are generated on a daily basis. This suggests that 90% of existing data was created in just the past two years.[15] Managing data can be challenging, whether you are:

- collecting and using data as part of your business model
- trying to limit ways that your customer (or employee) data is being used
- striving to comply with various data protection laws and regulations or
- engaging in all of the above.

The Federal Trade Commission (FTC) has long advocated the notion of "privacy by design," including building security into programs, apps and connected protects on the front-end, rather than after the fact[16]. Keeping this idea in mind can be helpful when implementing your data strategy.

## 2. Setting your Data Strategy

The first step in setting a data strategy is to identify what data you actually need to collect in order to conduct business. In particular, what personally identifiable information, or PII[17], if any will you be collecting? Because the collection and

---

[15]IBM, *Bringing big data to the Enterprise*, available at http://www-01.ibm.com/software/au/data/bigdata/

[16]*See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 19-22 (2015) (staff report), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november- 2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[17] The U.S. Department of Labor defines PII as "[a]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

storage of most sensitive data is often subject to federal and state regulation[18], a general rule of thumb is to only collect the data you really need in order to perform the services or provide the products you are offering.

By way of example, when I opened my own information technology law firm just over two years ago, I determined that I did not need to collect, use or store any client credit card information. For seminars that my firm has conducted that include online registration, I have utilized various service providers to handle the attendant payment transactions[19]. By doing so, my firm does not have access to that data and is, therefore, not subject to the corresponding regulations or industry standards, such as PCI Security Standards[20].

Once you have identified the data you will be collecting, the next step is to determine how you will be handling the data and, in particular:

- use of the data in furtherance of providing the services or products, or otherwise
- storage of the data, including where and in what medium
- sharing or not sharing with employees, business partners and others
- protecting the data, including the types and levels of security measures and
- ultimately, disposition of the data, including how long particular information should be maintained.

## 3. Establishing Data Practices

After identifying the data you are collecting and determining the ways you are handing the data, it is time to establish appropriate and practical practices and procedures that take into consideration the manner and type of data involved.

In my law practice, I decided to primarily keep electronic files instead of the more traditional hard copy files. This decision makes sense, given the nature of my practice and the type of information involved, such as, client communications, contract drafts, online terms and policies, presentations and articles. By contrast,

---

[18] If you are doing business outside the United States, the data protection laws of other countries may also apply. Such laws are generally much more stringent that those in the U.S., so it is important to consult with a lawyer in the countr(ies) in which you plan to conduct business.

[19] See, for example, Benchmark, http://www.benchmarkemail.com and Eventbrite, https://www.eventbrite.com

[20] See the PCI Security Standards Council for more information: https://www.pcisecuritystandards.org/merchants/

an estate planning lawyer whose practice involves wills, trusts and related documents may chose to maintain hard copies of these documents rather than (or in addition to) electronic versions.

It is also important to understand that your data handling activities should be consistent with any specific laws and regulations that apply to your specific industry or the type of data you are processing, such as Graham-Leach-Bliley Act (GLBA), a federal law that requires a privacy policy and annual notice to customers and consumers[21] and the Health Information Portability And Accountability Act (HIPAA) that mandates privacy policies and practices with respect to protected health information[22].

## 4. Aligning Business Partners

A few years ago, the Royal Bank of Scotland (RBS) received a call from a gentleman who advised them that he had just purchased a server on eBay that contained personal information of over one million RBS customers. Once RBS verified that the call was not a hoax, the bank was able to retake possession of the service and determined that it had been sent to its data archiving vendor who had apparently not wiped the data from the server before disposing of it[23].

Avoiding this type of embarrassment and potential liability should be a top priority. Once you've established your data handling practices, don't overlook the practices of any subcontractors or business partners with whom you are sharing data, particularly, PII or PHI. For example, if you state in your privacy policy that you do not share information with third parties for marketing purposes, make sure that your subcontractors don't do so, either.

## 5. Maintaining Transparency

The FTC's "privacy by design" initiative also recommends greater transparency over business' collection and use of consumer information[24]. If you are collecting

---

[21] For more information on GLBA, see the Federal Trade Commission's Guidance available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

[22] More information on HIPAA is available at http://www.hhs.gov/ocr/privacy/

[23] For more information about this incident, see BBC News, *"Bank customer data sold on eBay* (Aug. 26, 2008) http://news.bbc.co.uk/2/hi/uk/7581540.stm

[24] FTC Commissioner Brill recently spoke on this topic at Carnegie Mellon University. The text of her speech is available at https://www.ftc.gov/public-statements/2015/01/its-getting-real-privacy-security-fairness-design-internet-things-keynote

sensitive information from customers, such as credit card numbers, social security numbers or other PII, a privacy policy should effectively notify a customer of what information you are collecting, how you share it and related topics like how a customer can update the information you have collected.

Affording customers an easy "opt out" is a good practice. A nice example of a clear opt out is that used by AddThis.com. The site contains the following statement, followed by a large "OPT OUT" button:

"We believe that delivering targeted and relevant advertising enhances your internet experience. We collect non-personally identifiable information from many of the websites in which AddThis is enabled and use that information to deliver targeted advertising on those websites as well as other websites you may visit.

If you prefer that we do not collect non-personally identifiable information about your website visits for the purpose of delivering targeted advertising, you may opt out by clicking on the "opt-out" button below."[25]

In summary:

- Identify the data you need to collect in order to provide your products or services
- Determine how you will collect, use, store, share, protect and dispose of the data in formulating your data management strategy
- Keep an eye on compliance with applicable federal and state (and international) data protection laws
- Establish practices, policies and procedures consistent with your actual data handling practices
- Exercise due diligence to confirm that your subcontractors and other business partners have consistent data handling practices
- Strive for transparency in your stated privacy policies
- Consult necessary experts, including information security professionals and lawyers to implement your data management strategy

## D. Controlling Digital Assets

This final section includes discussion of maintaining control over your business' key digital assets. Specific topic include:

- The role of digital assets in today's business environment

[25] http://www.addthis.com/privacy/opt-out

- Differentiating business and personal accounts
- Recent lawsuits over digital assets
- Keys to keeping control over your digital assets

## 1. We live in a Digital Age

Almost every business, regardless of industry, relies on digital assets, either to deliver goods or services, marketing, or back office administration. Here are just a few examples:

- Email accounts
- Cloud-based accounts such as Salesforce[26], Dropbox[27] and Sharepoint Online[28]
- Web sites and blogs
- Online banking and bill-paying
- Social Media presence on Facebook[29], Linked In[30], Twitter[31], YouTube[32] and others

Because digital assets are important to your business, some thought should be given to how best to establish and maintain control over these assets. While the remainder of this article focuses on social media accounts for illustration purposes, other types of digital assets are equally or perhaps even more important and can be handled in the same or similar ways.

## 2. Business versus Personal

The particular social media platforms that you participate in are up to you and your marketing team to decide. Once you have chosen platforms, the next

---

[26] Salesforce is a customer relationship management (CRM) platform found at https://www.salesforce.com

[27] Dropbox, a file sharing platform, is located at https://www.dropbox.com

[28] Microsoft offers a host of cloud-based business services through Sharepoint Online. More information is available at https://products.office.com/en-us/sharepoint/sharepoint-online-collaboration-software

[29] https://www.facebook.com

[30] https://www.linkedin.com/nhome/

[31] https://twitter.com

[32] https://www.youtube.com

consideration should be whether your presence on those platforms will be strictly business-related or some combination of business and personal. For highly regulated industries, like banking and broker-dealers, the strictly business approach may make the most sense. Broker-dealer employees may find that setting up and using a "business" Facebook page too restrictive to be of use.[33] On the other hand, Internet-based businesses, such as Buzzfeed[34], may encourage the use of social media by its employees to advance business objectives[35].

For my own information technology law firm, I chose to set up business pages on Facebook, LinkedIn, Twitter and YouTube. Each are use strictly for business purposes and do not include personal content[36]. That said, part of my marketing strategy is, often, to share the content from the business pages on my personal Facebook, LinkedIn and Twitter pages.

Another major consideration is who will have administrative access to the business pages. You can designate either a single administrator or, perhaps, co-administrators who are then each able to access, modify and update the pages. Choose your administrators with care. A number of businesses have unwittingly found themselves engaged in protracted and expensive litigation over the ownership of social media accounts.

## 3. Litigating Social Media Account Ownership and Control

***Whose Twitter Account Is It Anyway?*** Noah Kravitz was a product reviewer and video blogger for his employer, PhoneDog. He used a Twitter account in his job with the handle @PhoneDog_Noah. Kravitz left his employment at PhoneDog and changed the Twitter handle on the account to @noahkravitz. In 2011, PhoneDog filed a lawsuit against Kravitz, claiming breach

---

[33] Broker-dealers and their representatives are subject to rules and regulations of the Financial Industry Regulatory Authority ("FINRA") and the U.S. Securities and Exchange Commission ("SEC"), including rules specifically regulating methods and types of communications. The inter-active, real-time nature of social media can make compliance with such rules challenging at best. More information about these regulatory bodies is available at http://www.finra.org and http://www.sec.gov

[34] http://www.buzzfeed.com

[35] In February, 2015, @leyawn combined, then tweeted 50 buzzfeed employees' Twitter bios into one block of text. See the tweet at https://twitter.com/leyawn/status/567799456469614592

[36] See, for example, the Ossian Law P.C. YouTube Channel at https://www.youtube.com/channel/UCZUckirsXGhjX2ZY7d-Ceiw

of confidential information and theft of trade secrets[37]. Shortly before the case was set to start trial, the parties entered into a confidential settlement. It is therefore unknown whether any money was exchanged, but we do know that Kravitz kept the Twitter account in question[38].

***But I Founded the Company!*** Linda Eagle was a founder and executive of Edcomm, Inc., a banking education company. In 2008, She set up a LinkedIn account, acted as co- administrator and used it for Edcomm business. The company was acquired in 2011 and, ultimately, Eagle was let go. Subsequently, when she tried to access the LinkedIn account, she found that the password had been changed. Eagle filed a multi-count lawsuit against the new owners to regain access to the account, including claims of conversion and tortious interferences. The company filed a counterclaim, asserting that the account belonged to the company. The case went to trial where Eagle asked for damages of $248,000. The court found that Eagle couldn't prove damages with reasonable certainty. At the same time, the court noted that the company had adopted no policy on whether LinkedIn accounts were the property of the employer or employee[39].

***Are LinkedIn Contacts "Trade Secrets?***" When David Oakes left his job at Cellular Accessories For Less to work for a competing business, he took his LinkedIn contacts. In 2014, Cellular Accessories filed suit against Oakes and his new employer, Trinitas, alleging that Oakes' LinkedIn contacts were trade secrets. Oakes moved to dismiss the claim, stating that LinkedIn contacts are "viewable to any other contact he had on LinkedIn" and, therefore, do not meet the criteria of trade secrets. The court denied the motion and allowed the claim to proceed, holding that there was a question of fact as to whether or not Oakes' LinkedIn profile was public or private[40].

---

[37] More information about the lawsuit is available at http://www.dmlp.org/threats/phonedog-llc-v-kravitz

[38] Kravitz now has 20,700 Twitter followers. https://twitter.com/noahkravitz

[39] A copy of the court's decision is available at https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/AdvertisingLaw@manatt/Eagle-v-Morgan.pdf

[40] The court's decision on Oake's motion for summary judgment is available at http://www.employmentmattersblog.com/files/2014/09/Cellular-Accessories-v-Trinitas-Order.pdf

In an unrelated case earlier this year, a federal court in Illinois held that membership of a private LinkedIn group may be a protectable trade secret, but the communications within the group are not.[41]

***Even in Bankruptcy!*** In another recent case, a bankruptcy court in New York held that social media accounts were assets of the bankrupt corporation rather than the owner's personal property. The court cited that the account was linked to the company's website, was used to promote the company's products and that other employees besides the owner posted status updates[42].

## 4. Steps to Keeping Control

Avoiding these types of disputes should certainly be a goal for any business. Here are some steps that can help to protect your key digital assets:

- Establish and update an inventory of digital assets
- Carefully choose and designate co-administrators
- Address ownership and control with employees using appropriate corporate policies, such as social media, external communications, mobile device management and other applicable policies
- Include protection of digital assets in exit interview checklist/procedures

Of course, consulting with your own attorney on how to maintain control of your business' digital asset is a must.

---

***THIS ARTICLE IS INTENDED TO PROVIDE GENERAL INFORMATION AND IS NOT OFFERED, NOR SHOULD IT BE RELIED ON, AS LEGAL ADVICE. YOU SHOULD CONSULT YOUR OWN ATTORNEY OR OTHER LEGAL REPRESENTATIVE BEFORE MAKING ANY DECISIONS OR TAKING ANY ACTIONS WITH LEGAL RAMIFICATIONS.***

---

[41]The decision in CDM Media USA, Inc. v Robert Simms is available here: http://www.gpo.gov/fdsys/pkg/USCOURTS-ilnd-1_14-cv-09111/pdf/USCOURTS-ilnd-1_14-cv-09111-0.pdf

[42]More information about the decision is available at http://www.abfjournal.com/articles/social-media-accounts-bankruptcy-court-ruling-sets-precedent/