PARTRIDGE SNOW & HAHN LLP

Bringing Your Business Online

The COVID-19 pandemic has forced many businesses online in order to survive. In many cases, businesses had no plans to be online. Others were forced to move online more quickly than planned. In order to assist these businesses, we have prepared a series of articles discussing some of the more important legal issues to address when moving your business online. **Website Terms** *discusses online terms and conditions to protect your business.* **Privacy Policy** *discusses how your business collects, uses and discloses personal information of others.* **Third Party Content** *discusses the risks of copying photos, music, videos, and other content created by third parties onto your website.* **E-Commerce Policies** *discusses e-commerce policies that a website selling products or services should have in place.* **Creating Enforceable Contracts** *discusses the safest method to ensure that you can enforce your online terms and conditions protecting your business.* **Written Information Security Programs (WISPs)** *discusses several reasons why it is important for all businesses to prepare a WISP and to keep it updated.* **Protecting Your Brand** *discusses the process of selecting and protecting your brand.* **Cyber Insurance** *discusses the importance of finding the right cyber insurance policy for your business.*

Website Terms

Job one is to get the online technology up and running. Then there are some legal issues to which you should pay attention to protect your business. For most businesses, these can wait until after you get your business up and running (all while balancing home schooling and grocery obligations). But these are all issues that you *should* address once you have had a chance to catch your breath.

One of the most important items that your website needs are “terms of use” (also known as “terms and conditions” or “terms of service”). These terms do not replace your ordering, sales and delivery terms. Rather, they govern the relationship between the operator of the website (your business) and the users of the website and its content.

There are several different kinds of terms, depending on the type of business you are operating.

The most common are:

Basic Terms of Use

For basic websites that only offer information about the business, the terms generally will provide that the content on the site is covered by copyright laws, that the content cannot be used for commercial purposes by others, and contact information for the business.

E-Commerce Terms and Conditions

For sites that allow users to create accounts, that sell products and services, or that allow others to post content or comments, further provisions should be added. These terms include

- provisions governing the accounts;
- provisions describing how accounts may be terminated;
- terms of sale;
- what types of payment are accepted;
- how payments will be made;
- how deliveries will be made.

If third party comments and content are allowed, the terms also will need provisions regarding copyright policies, and how others can submit claims of copyright infringement.

Apps/Terms of Service

For websites that provide services directly (sometimes known as "Software as a Service" or "SAAS" websites), additional terms are required. These terms discuss the rules of how the website can be used and limit the website operator's liability for such use. If an application (or "app") for tablets or wireless phones is connected to the website, these terms also generally will provide licensing terms and requirements for use of the app.

It is tempting to just copy the terms from another website, especially when you are rushed for time. However, there is danger in doing this, as the terms on another site may omit a provision that you need to protect your site or, may contain provisions with which your site does not comply. Either way, you could be subjecting your business to unnecessary liability. It is much safer to construct your own agreement tailored to your business.

Privacy Policy

The next element to consider is a privacy policy. A privacy policy is a document that discloses:

- What personal information the business collects from individuals online;
- How the personal information is collected;
- How the business uses the personal information;
- How and to whom the business discloses the personal information;
- How the business manages and stores the personal information that it collects; and
- How the individuals can correct the personal information.

The definitions of "personal information" vary, but generally the term covers anything that can be used to identify an individual or access his or her financial accounts. Examples include an individual's name, address, date of birth, marital status, credit card information, bank account

information, and health information. Businesses that do not collect any personal information, or that only collect information from other businesses and not from individuals, probably do not need a privacy policy.

The most important thing about a privacy policy is that it reflects the business's actual practices. The Federal Trade Commission and state attorney generals have brought enforcement actions and imposed fines and monitoring orders against businesses that have not followed established privacy policies. This also means that the policy needs to be updated whenever the business's collection, usage and disclosure practices change over time.

There is no one law that governs privacy policies or that prescribes what to include. Federal laws impose specific requirements for businesses in the health care and financial services industries and for businesses that collect personal information about children. A few states also have laws requiring privacy polices if a business collects personal information from residents in those states. If a business is targeting residents of the European Union (EU), then the requirements of the EU's General Data Protection Regulation (GDPR) also apply. Certain popular Internet tools, such as Google Analytics and Facebook Lead Ads, also require privacy policies.

It is tempting to just copy a privacy policy from another website, especially when you are rushed for time. However, there is danger in doing this, as the other company's privacy policy may not address laws that apply to your business. Even worse, the other company's information collection, usage, security and sharing policies are probably different from those of your business. You expose your business to unnecessary liability because you will not be following "your" privacy policy. It is much safer to construct your own agreement tailored to your business.

Third Party Content

Another area to consider relates to when you can and cannot use someone else's content on your website. As a general rule, one cannot use or copy content you find on the Internet without permission. This rule applies to all creative content: text, videos, photographs, maps, cartoons and drawings, and music. This is true even if the content or the website does not have an explicit copyright notice or copyright symbol © (the letter c in a circle). Federal copyright law protects the creator of the content from the use of that content by others without permission, whether or not the content contains a copyright notice when published.

Posting an unauthorized copy of someone else's content on your website often proves to be expensive. This practice can expose you to charges of copyright infringement, even if you did not intend to infringe, and even if the content was added by your web designer in creating your website. In a lawsuit, there are numerous ways compensation may be pursued. The copyright owner can request that you pay "actual damages," which are often the amount that the owner would have charged to license the content. In some cases, as an alternative, the owner can ask to court to award "statutory damages" in an amount between $750 and $30,000 without any requirement to show actual damages. In addition, you may have to pay the owner's legal fees, in addition to your own for defending the lawsuit.

Some content is acceptable to use. For example, U.S. government works, including laws, regulations, opinions, reports, photos and videos, are not protected by copyright and are free to use by anyone. But that does not mean that everything on a federal government agency website is free to copy. Someone other than a government employee could have taken photos and then

given the agency permission to use the photos on the website. Content first published in 1924 or earlier, unpublished content created by unknown authors prior to 1900, or by authors who died in 1950 or earlier, also are no longer covered by copyright and are free to use. There are also a number of websites that offer "public domain" photos, graphics or music that is available for use for free or a nominal fee. It is much safer to use this content than to copy content from another website.

Another practice that is generally acceptable is to link to the content on another site where it appears. This enhances the value of your website by directing the user to useful content. But there are some traps, even with linking. Be careful to provide just a link that directs the user to the other site, but does not repeat the content found there. In addition, you should review the terms and conditions of any site to which you link in order to determine whether the site allows linking.

E-Commerce Policies

Websites that sell products or services also need to prepare and disclose their business policies regarding returns and refunds, shipping, payment options, and order cancellations and refunds. It is tempting to copy these polices from other websites. The danger, however, is that the other websites may not have exactly the same policies as your company. In so doing, you could be subjecting your business to unnecessary liability.

Depending on the nature of your business, some of the policies and terms you should consider are:

- **Return and refund policies** --- Businesses that sell products online generally need a return and refund policy to govern when customers can return products. Some of the questions you may want to address in this type of policy are: Under what circumstances can the customer return the product (any reason, only if defective, all sales are final, etc.)? What are the time limits? Are there other conditions (must be in original packaging, must have original receipt or proof of purchase)? Who pays for return shipping? Do you want to provide a store credit or, a refund or partial refund? Is there a restocking fee?

- **Shipping policies** --- Shipping policies generally let the user know what shipping options are available, how much each option will cost, and when the shipment will arrive. The policy can also address any restrictions on shipping and delivery, such as not delivering to post office boxes or to certain states or countries, or that an adult at least 21 years old needs to sign for the delivery.

- **Payment terms** --- If the payment terms are not in your terms and conditions, you will also need a separate policy setting forth the terms. This policy generally addresses the following questions: What types of payment methods are accepted (credit cards, PayPal, purchase orders, etc.)? How will late or missed payments be handled, if you do not collect payment in full up front? For subscription services, when and under what circumstances can you suspend or terminate the subscription for non-payment? Does a customer get a refund for early termination? When and under what circumstances can you change the prices or fees (at any time, upon 30 days' notice)?

- **Cancellation and refund policies** --- If you are a business that takes reservations (hotel, restaurant, online classes), cancellations at the last minute can cost you time and money, and lost profits. Some of the questions you may want to address in such a policy are: How can the customer cancel the order, if at all? Are there time limits? When does the customer have to inform you in order to cancel? How do they inform you? Do you want to provide a refund or partial refund? Do you want to provide a store credit, and, if so, how long is the credit good for (there may be laws in your state that apply to this question)? Are orders transferrable if you are not going to provide a refund?

Creating Enforceable Contracts

Online businesses spend a lot of time and money preparing terms and conditions for their websites. These terms explain the rights and obligations to customers, and are supposed to protect the businesses. Yet, we see disputes time and time again over whether or not the online terms and conditions can be enforced against a user.

This isn't rocket science. If followed, basic contract law principles should maximize the likelihood that your terms can be enforced. These principles are not always followed, however. The result has been scores of lawsuits, many involving large companies with extensive legal resources, whose users successfully have challenged the enforceability of the online terms and conditions. Given that each side in a lawsuit can easily spend tens or hundreds of thousands of dollars, it makes sense to take steps to avoid this risk.

The best way to create an enforceable agreement is with what is commonly called a "click through" or "check the box" agreement. If your website is an e-commerce site, you have a couple of options:

- At the point of purchase, directly above the "Purchase" button, add a conspicuous sentence that says "By clicking the "Purchase" button, you agree to our terms of use" with a hyperlink to the terms of use page or document.
- Even better, at the point of purchase, directly above the "Purchase" button, you could add a blank check box (that the user needs to check) with the language" By checking this box, I acknowledge that I have read and that I agree to the terms of use" with a hyperlink to the terms of use page or document.

Even if your website is not an e-commerce site, it is relatively easy to form a "click through" agreement if you have an account registration process. Directly before the point where the user completes the registration, add a conspicuous sentence like "By creating an account, you agree to our user agreement" with a hyperlink to the user agreement page or document.

In both cases, you need to make sure that the user can print or save the terms of use if desired. You also need to make sure that the customer cannot complete the purchase unless the box is checked if you use that approach. For evidence purposes, your business also needs to maintain reliable records to show the agreement's terms on any specific date (for situations where the terms may change over time and the user disputes which version he or she agreed to) and what interactions (for example, check the box, clicking a button, etc.) were required technologically for the user to manifest his or her acceptance on that date.

Written Information Security Programs (WISPs)

In the context of an online business, a WISP is not a small bunch of hay or straw. If your business has employees or customers in Massachusetts or Rhode Island, you must have a written information security program (WISP). Many other states have similar requirements.

If your business (wherever located) collects, stores or uses personal information about an individual, many states have laws that legally require you to: (a) develop, implement and maintain a comprehensive WISP; (b) implement physical, administrative and extensive technical security controls, including the use of encryption; and (c) verify that any third party service providers that have access to this personal information can protect the information. “Personal information” can be a first name, last name and the last 4 digits of a social security number, credit card number or bank account number of a customer.

Business leaders need to understand that the WISP is a “program,” not a “policy.” The WISP is intended to describe a system by which one runs the business on a day to day basis to safeguard sensitive information. Our experience with WISP’s is that some clients treat them like policies that they can have drafted and then throw in a drawer and never look at again. Some businesses have copied a WISP from a form found on the Internet, or a form provided by another company, but have not taken the time to customize it for their business. Other companies want to say they have a WISP, but do not actually make any operational changes to implement the purported security programs described in the WISP. This practice can be risky under state laws such as Massachusetts.

There are several reasons why it is important that all businesses prepare an information security program and update it regularly:

- WISPs help to reduce the risk of liability and adverse publicity should a data breach occur. State enforcement officials have pursued and obtained six figure civil judgments for violations of these regulations. In addition, the laws in some states require breach notices to state whether or not the company maintains a WISP;

- Some state laws, such as those in Massachusetts, require businesses to review their WISP’s at least annually. We see many companies who initially prepared information security programs but have not reviewed or updated their policies on a regular basis;

- Information security programs help with training employees in company policies and procedures with respect to confidential and sensitive information.

Protecting Your Brand

The process of selecting and protecting a trademark in the United States consists of two steps. First, is the mark available to use without the risk of infringing the rights of others? Then, how do you protect the mark from being used by others? Each step is briefly discussed in further detail below.

Availability

When you move your business online, your brand becomes more visible. . Before investing substantial sums in promoting the brand, it is a prudent idea to conduct one or more trademark

searches. These determine whether others are already using a mark, so you can avoid investing substantial sums in a mark in which you will not have strong trademark rights, or which you will have to change later. There are a number of ways to search, but the two most common are: (1) an online "screening search" of the mark submitted for registration to the U.S. Patent and Trademark Office (PTO); or (2) a broader search of the trademark records in addition to common law sources, databases, company name directories, trade publications, etc.

Because a search is not mandatory, it can be done before or after the applications are filed, or not at all, depending on your "risk-benefit" analysis. But it is always less expensive to undertake such a search than to have to rebrand and reprint physical marketing materials and reprogram websites and online marketing materials.

Protection/Registration

The most important marks or brands to protect vary from company to company. Typically, however, we recommend that the business protect the company name and logo, and any significant product or service brands, logos and tag lines.

Typically, rights in a trademark or brand in the United States are acquired by ***use of the mark*** on or in connection with providing goods or services in commerce, ***not by registration***. If you choose not to apply to register a mark with the PTO, you can rely on common law trademark rights, but only to the extent the mark is actually being used, and then only in the area or areas where the goods or services are marketed or offered for sale. This is why there can be more than one company with the same or similar names in different parts of the country.

Thus, trademark registration in the U.S. is voluntary. However, owning a federal trademark registration provides several advantages, including:

- Notice to the entire nation of your claim of ownership of the mark;
- A legal presumption that you own the mark and you have the exclusive right to use the mark nationwide on or in connection with the goods or services listed in the registration (except against anyone else who is using the same or similar name before the registration), which reduces the amount of time and money you need to be spending in proving these issues in a legal dispute;
- The ability to use the U.S. registration as a basis to obtain registration in foreign countries;
- The ability to use the U.S. registration as a basis to object to the registration of confusingly similar domain names;
- The ability to use the U.S. registration to register the brand with the Amazon Brand Registry.

One thing to note is that registration of a mark provides the owner with ***prospective*** protection only. You may then enforce your rights against users who adopt the same or a similar mark after you do. However, even with a registration, you generally will be unable to stop a prior user of a similar name or mark.

The process with the United States Patent and Trademark Office (USPTO) typically takes 10-18 months until a mark is registered. For most organizations, this means that you should consider

applying to protect only those marks of significant importance to the organization that are not "one-time" events or that are not going to change or be replaced frequently.

In many other countries, trademark rights are acquired by registration. This means that, if you are doing business or are considering doing business outside the United States in the future, you should consider applying to register the mark (at least in the most important countries). Otherwise, you could run into a situation where someone else has registered the mark and can prevent you from using the mark in that country.

If your business is only contemplating selling products or providing services locally, there is also the option of filing a trademark application at the state level. A state registration typically provides protection only within the geographic boundaries of a state. Filing for one or more state registrations is a cost-effective strategy sometimes for businesses just starting out that cannot afford the cost of a federal filing yet, or for businesses that are truly local in nature. One generally can apply to register a trademark in 2 or 3 states for about the same cost as a federal filing. After that, the nationwide advantages of obtaining a federal registration typically outweigh the cost disadvantages.

Until you actually receive a Certificate of Registration from the USPTO, you cannot use the registration symbol ® in connection with use of your mark in the United States. You can, however, use the designation ™ to inform the public of your claim of ownership. The ™ symbol has no legal significance but is commonly understood to mean that your company claims that symbol as a trademark. You can use this ™ symbol as soon as you start using the mark, even if you do not apply to register the mark at the state or federal level.

Cyber Insurance

Bringing your business online introduces new risks, including the need to have more *digital* data about your customers, such as credit card information, names, addresses, contact information, and purchase history. Some of that data may be stored on your company's computers, and some may be stored with a third party vendor in the "cloud."

All of this digital data is vulnerable to attacks by third parties who want to access it. Cyber attacks can cause harm to your business in a number of different ways. You will incur costs to investigate the cause of the attack and to recover data and systems, and may be forced to pay a ransom fee to "unlock" your company's data. In addition, after a cyber attack occurs, your business also may incur costs to investigate the breach, to notify customers and other third parties (such as regulators and attorneys general) if sensitive information is involved, and to defend and settle lawsuits involving claims that your company did not act properly in protecting the data.

A common misconception is that these cyber attacks only happen to large companies. In reality, attackers frequently target medium and small businesses, but you are less likely to hear about them on the news. A recent study reports that over 40 percent of all attacks occur at businesses with 100 or fewer employees. Small businesses are particularly at risk because they typically do not have access to the same level of resources as a large business to protect themselves.

Many companies are surprised to discover that their general commercial liability policies do not cover most types of cyber risks. Commercial general liability policies typically only cover bodily injury and property damage, not monetary losses, ransom costs, or regulatory fees and

expenses. In addition, coverage is often limited to losses caused by "tangible" means. Insurance companies typically consider data breaches to be "intangible" causes not covered by the policy. Most commercial general liability policies also include an exclusion for access to or disclosure of confidential information, and the resulting liability.

One important tool to reduce the risk is a cyber insurance policy. There are many differences among policies, so it is important to discuss coverage with an insurance broker or agent with experience in this area.

Here are some questions to ask when you are investigating cyber insurance policies:

- **What data does your business have, and where are you at risk for a cyber attack?** Most businesses have some data, such as credit card data or employee information, that can be compromised.
- **Does your policy have first party and third party coverage?** First party coverage pays for damages resulting from a breach of your company's computer system. Third party coverage pays for damages resulting from a breach of data you have given to a third party vendor. It is important that most businesses have both types of coverage.
- **What risks are covered and what risks are not covered?** Are these risks for which your business needs coverage?
- **What are the policy limits?** All policies will have limits on coverage and many will have sublimits on certain payments (for example, the costs of forensic investigations). Are the sublimits reasonable in light of the likely average cost to your business if a cyber attack occurs?
- **What are the policy retention (deductibles) amounts?** If the retention amount is very high, the insurance may not be of much benefit to your business except in extreme cases.

Defending against cyber attacks has become a cost of doing business for all businesses, not just large companies. The first defense is to have consistent policies and procedures in place that are followed by all employees and others who have access to confidential data. As a backstop, cyber insurance can be an important part of that defense for many businesses.

*Partridge Snow & Hahn Partner **John Ottaviani** has over 25 years of experience bringing businesses online and can provide the guidance needed to make the transition as painless as possible. He can be reached at **jottaviani@psh.com** or 401-861-8253. For more information visit **psh.com**.*

Partridge Snow & Hahn LLP's Response to COVID-19:
The world is a different place than it was a few months ago. Partridge Snow & Hahn's top priority is still and will always be to ensure that our clients receive the same exacting level of service, responsiveness and expertise that we have delivered for more than thirty years. For some time, all of our attorneys have been equipped with the capability to work remotely. We are taking advantage of that preparedness now. Our attorneys are working remotely to help protect our people and our communities.

We are fully equipped, fully engaged and ready to help you with all of your legal needs, whatever they may be. We will continue to be responsive and on top of the issues you bring to us. For current information and resources visit Partridge Snow & Hahn's COVID-19 Advisory Group page.