Why Audit Your Website?

If your online presence is important to your business then you already know.

Table of Contents

What is a website audit?

The answer to this question obviously depends on what is being audited. At the Digital Business Law Group (DBLG) what we mean by a website audit is a review of your online presence to ensure that it complies with all applicable law U.S. law, and where required, to international law as well. The audit usually encompasses drafting and/or reviewing your privacy policy and terms of service. However, if your site conducts commerce then it is likely we will need to draft/review your advertising, subscription and other similar agreements, depending on your business model. You can think of an audit as an insurance policy; one that reduces the risks of doing business online. The risks that an online business faces are, in general, similar to risks faced by brick and mortar businesses, except that the virtual world presents additional risks that are unique to the Web. From a legal perspective, online risks tend to fall into two major categories, compliance and security. The two are closely related and in some cases interchangeable. A risk management strategy that addresses both is critical to mitigating legal liability, but even more importantly, to maintaining your business' reputation value.

One important point to remember is that compliance and security cannot be addressed solely with the appropriate "legalese." Both require that special attention be paid to developing and implementing the underlying business processes that support the legal language. Without the processes underpinning the language, it will be difficult for a lawyer to make a reasonable, let alone compelling, good faith argument on your behalf. The Federal Trade Commission's (FTC) guidance of "say what you mean and mean what you say" gets at the heart of the matter. Although the type of processes required will vary with the size of the business, even small online businesses cannot afford to be oblivious to process issues. At DBLG we understand that many online businesses are completely overwhelmed by regulatory requirements. We provide guidance and resources that allow you to take a pragmatic, common sense approach regarding effective online risk management, depending on your unique requirements.

What laws apply online?

The short answer to this question is that, in general, most laws that apply to brick and mortar businesses apply to an online business. That said, the Web is a kind of jurisdiction of its own, not in the classical sense, but rather in the sense that some laws directly target online activities. The following list is not exhaustive but will give you a feel for what is out there:

- The Digital Millennium Copyright Act (DMCA)—copyright safe harbor for online websites.
- Communications Decency Act (CDA)—section 230 provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by others.
- Children's Online Privacy Protection Act (COPPA)—applies to the online collection of personal information from children under 13.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)—sets national standards for the sending of commercial e-mail and requires the FTC to enforce its provisions.
- Fair Credit Reporting Act (FRCA)— regulates the collection, dissemination, and use of consumer credit information, including the Red Flags Rule which targets the prevention of identity theft.
- U.S. Safe Web Act of 2006—enhances FTC enforcement against illegal spam, spyware, and cross-border fraud and deception.

- Health Insurance Portability and Accountability Act (HIPAA)—requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers; it helps people keep their health care information private.
- Graham-Leach-Bliley Act (GLBA)—requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties.

You can add to this list the Federal Copyright, Trademark and Patent Acts as well as an increasing number of state laws that directly target online businesses.

Why do you need a terms of service agreement?

The terms of service (TOS) agreement (sometimes referred to as a terms and conditions agreement) establishes the terms and conditions that users must agree to before accessing/using your website. It is your contract with end users that controls: 1) acceptable conduct on the site; 2) rights regarding content on the site; 3) the services provided by the site; 4) legal liability, warranties, indemnification, termination, jurisdiction, venue, etc.; and 5) compliance with applicable law.

The TOS should be posted conspicuously on your site. We usually recommend that it be placed on the footer of every page, along with your privacy policy and copyright notice. For sites that allow users to register then the recommended practice is to force users to click an "I Agree" button, after displaying both the TOS and the privacy policy. As Internet use has exploded, courts are beginning to pay close attention to TOS agreements, and how they are modified (i.e. how notice is provided to users when "material" modifications occur).

DBLG also recommends that sites track which version of the TOS and privacy policy a user registered under, for both notification and litigation purposes—only a few sites do this today; however, it is an emerging best practice.

Why do you need a privacy policy?

There is probably no hotter issue online than the protection of consumer privacy. The purpose of a well written privacy policy is to let your users know what information you collect, why/when/how you use the information, and what safeguards you have in place to protect it. The general rule from the FTC, and other Federal agencies, is that you must implement reasonable and appropriate data security measures. What this means in practice will vary by industry and type of business. That said, special precautions are always required when a business transmits, processes and stores personally identifiable information (PII). PII refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

PII may include, but is not limited to, the following kinds of data:

- Full name (if not common)
- National identification number (SSN)
- IP address (in some cases)
- Vehicle identification number (VIN)

- Driver's license number (DLN)
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Birthday
- Birth Place

The FTC recommends a five step plan to protect personal information in general, but especially PII:

1. Take Stock: Essentially, perform an assessment/inventory of where personal info is stored in your organization.
2. Scale Down: Keep only what you need for business purposes or for government reporting purposes.
3. Lock It: Protect the information you keep. Be cognizant of physical security, electronic security, employee training, and the practices of your contractors and affiliates.
4. Pitch it: Properly dispose of what you no longer need. Make sure papers containing personal information are shredded, burned, or pulverized so they can't be reconstructed by an identity thief.
5. Plan Ahead: Draft a plan to respond to security incidents. Designate a senior member of your team to create an action plan before a breach happens.

Recent high profile cases have demonstrated that Federal agencies are willing to impose significant fines when a data breach occurs. Having the appropriate privacy policy and processes in place will not eliminate legal liability, but it will certainly contribute to preventing and mitigating it. Privacy and security will continue to be front burner issues both nationally and internationally. The States are also getting in on the act with their own online consumer protection/data breach laws. Notification to consumers when a data breach occurs is becoming a universal requirement.

Healthcare providers and facilities (collectively "providers") in particular need to be aware that the recently enacted HITECH Act has transformed HIPAA from a paper tiger into an electronic beast. Providers therefore need to be concerned with not only protecting any PII collected, but also with meeting the requirements of HIPAA's Privacy and Security Rules regarding protected health information (PHI). The HIPAA Security Rule has largely been ignored because few providers had migrated to electronic health records ("EHRs"). That is all about to change with the financial incentives for EHR adoption provided in the HITECH Act.

Many healthcare providers are starting to make the move online. That is really not surprising since this move (like in every other industry) appears inevitable. Providers that were once tepid about making the move online are now going to be in a hurry to get there, since they will see the advantages that more nimble competitors are obtaining, like the small matter of getting paid their EHR incentives. However, many providers are unaware of the legal compliance issues that they may face as they go online. For example, section 164.520(c)(3) of HIPAA's Privacy Rule states as follows (paraphrasing): "*A covered entity (CE) that maintains a website must make the notice prominently available on its website. A CE may provide notice via email if the individual has agreed to such notice and other requirements of this section are met.*" This notice reference is to a provider's HIPAA Privacy Notice and is not a reference to the typical privacy policies found on most websites. Of course a provider could place the HIPAA notice there, but then the issue becomes whether or not the "prominently available" requirement has been met?

In addition, HHS' recently promulgated Interim Final Rule on Breach Notification raises the stakes even higher for providers. If unsecured PHI is breached then a provider may need to notify HHS, the local media, and each individual patient whose PHI was compromised. In addition to a compliance violation, this kind of notoriety could drastically impact a provider's business. How much is a provider's reputation worth?

What other agreements do you need?

Depending on the unique aspects of your online business you may need any number of other kinds of agreements. Most small online businesses do not recognize the need for these until they become the target of a legal dispute, or an enforcement action by a government agency. It is understandable why these needs go unmet. Start-ups are struggling for their economic survival and often cannot afford anything but the necessities when it comes to legal services. The problem is that these needs almost never get revisited once the business becomes cash flow positive. The following kinds of agreements are representative of what many online businesses fail to establish:

- Subscription & membership agreements
- Advertising agreements
- Intellectual property agreements
- Affiliate & reseller agreements
- Email marketing agreements
- Website/software development agreements

This list is not exhaustive, but should give you a sense of what other types of agreements may be required. The more successful an online business becomes, the more likely it is to be the target of a lawsuit and/or a government enforcement action.

Are these agreements enforceable?

The answer to this question depends on a number of variables, including how the agreement was drafted, how the acceptance of the agreement was acknowledged, and what court is interpreting it. For agreements that do not require an affirmative acceptance (i.e. "browse wrapped" agreements) it will depend on whether the end user had actual or constructive notice of the agreement. Another important consideration is how to notify users when material modifications are made to the agreement, and where appropriate, how to ensure that users have affirmatively accepted the modifications.

Summary

Although, conducting a website audit will not eliminate your legal liability, having the appropriate agreements in place, and the business processes that underpin them, will ensure that you are protected to the maximum extent allowed by law. A website audit is a kind of insurance policy for your online business. Privacy and data security issues will continue to receive increasingly more attention from consumers and from federal and state enforcement agencies that act on their behalf. More is at stake than can be measured by fines or from damages payable from the loss of a lawsuit. How much is your business' reputation worth?