

## **Beyond the Homepage: 10 Points to Consider When Building or Updating a Company Website**



## **Beyond the Homepage: 10 Points to Consider When Building or Updating a Company Website**

Published April 11, 2016

Most people might agree that it is more interesting to focus on the design elements of a website that customers see, but it is crucial to structure a company's online presence so that the website meets the current legal requirements and can evolve with the changing legal landscape. The impact of not doing so can be staggering. An underdeveloped website structure or omitted functionality, will require far more time to fix than had the project been strategically planned from the beginning.

It can seem like there are more questions than solutions: If users' personally identifiable data is collected through the website, what do you plan to do with it and how will you protect it? Do you plan to advertise or market your products to users once you have their contact information? Do you plan to sell your products through an online store? How do you set up an online store? Do you have intellectual property assets that you want to protect? Do you need a privacy policy or terms of use? Will your users be located in the United States or in other countries?

To make matters more complicated, California has numerous laws, regulations, and standards that may be implicated depending on what you plan to do with your website and the services that you will provide. And, the laws are changing . . . rapidly. For example, California's data breach notice requirements contained in California Civil Code sections 1798.82 (for businesses) and 1798.29 (for agencies) were modified effective January 1, 2016. In February of 2016, the European Commission and U.S. Department of Commerce reached agreement on a new framework governing the movement of data between the European Union and the United States, dubbed the "EU-US Privacy Shield" which comes on the heels of the invalidation of the EU-US Safe Harbor that had existed for over 15 years. Additionally, in March of 2016, the California Court of Appeals for the Second District and the U.S. Court of Appeals for the Seventh Circuit both opined on the enforceability of websites' browserwrap and clickwrap terms of use.

Given the complexities of the legal environment, there are 10 things to keep in mind as you create, or look to update, your company's website:

1. *Have a Privacy Policy.* If you collect any user data through your website (including, without limitation, name, email address, date of birth, physical address, or payment information) make sure you have a privacy policy that complies with California's requirements. (See California Civil Code section 1798.80 *et seq.* and California Business and Professions Code section 22575 *et seq.*) For example, California law requires companies to disclose to users if behavioral tracking is used and how the user might go about opting out of such tracking. Additionally, if you transfer or receive personally identifiable data from individuals in foreign countries, make sure that you are aware of, and can comply with, the applicable local laws and regulations of the foreign jurisdiction.
2. *Protect the Data.* Set up technical, physical and administrative controls to protect users' personal information, and adopt policies and procedures for what to do in the event of a data breach. Data breach responses depend on the type of data involved so take the time to determine what kind of data your company will have in its possession.
3. *Protect Your Intellectual Property.* Go through the effort of copyrighting and trademarking your company's intellectual property assets that should be protected. Also, if you allow users to submit contributions (*e.g.*, through a forum or comment section) or use third party content on your website, consider registering a copyright agent to protect yourself under the Digital Millennium Copyright Act's Safe Harbor provision if someone claims content on your website is infringing their intellectual property rights.
4. *Website Terms of Use.* If your intellectual property assets are accessible or if you have functionality on your website that allows user contributions on forums or other postings, make sure that you have terms of use that govern use of your website. Two methods are generally used obtain users' consent to terms of use. A "browserwrap" terms of use appears as a link on the website that does not require a user to look at it or click through it because a user accepts the terms by using the website. Alternatively, a "clickwrap" terms of use requires the user to access or scroll through the terms and click a button to manifest assent. As mentioned above, the California Court of Appeals for the Second District recently held that a browserwrap version needs a "conspicuous textual notice" near the hyperlink to the terms of use to put users on notice of its terms. (*Long v. Provide Commerce, Inc.* (Mar. 17, 2016, B257910) \_\_ Cal.Rptr.3d \_\_.) The appellate court found that the browserwrap terms of use, without something more that puts the users on notice of its terms, will not be binding on users.
5. *Payment Processing.* If you operate an online store on your website, make sure you, or your payment processor, comply with applicable data security and processing standards such as the Payment Card Industry Data Security Standard.
6. *Electronic Transactions.* If you do any transactions electronically, make sure your transactions comply with the Uniform Electronic Transactions Act (codified in California Civil Code section 1633.1 *et seq.*) to ensure that the transactions are enforceable. Generally, the user must be able to consent to transact electronically, to review and edit the transaction prior to submission, and to print or save a copy of the transaction.
7. *Vet Your Vendors.* If you use a third party hosting vendor, or the "cloud," make sure the hosting vendor's security standards align with the kind of data you will be storing with the vendor. For example, if you will send Protected Health Information (as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")), to the vendor, make sure the hosting vendor is HIPAA-compliant and will sign a Business Associate Agreement. If you host personally identifiable information as defined in applicable law, make sure the hosting vendor has recently, and annually, undergone a security audit like the Statement on Standards for Attestation Engagement ("SSAE") 16.) Make sure you also have written agreements with your vendors and that the vendors are obligated to protect the data.
8. *Website Development.* If you contract with a third party to create your website or some custom functionality for the website, be sure to enter into a written agreement that clearly states who owns the work or the different parts of the work and who owns the different types of data flowing through the website (including the list of users and personal information).
9. *Marketing and Advertising.* If you will be sending marketing or advertising communications to users, make sure you either have their permission to send these types of communications, or a process so that users can opt-out of these communications if they so desire.
10. *Accessibility.* Consider the functionality and purpose of your website and whether accessibility features may be

required to comply with anti-discrimination laws or otherwise appropriate.

As this list shows, the issues related to websites are varied and numerous. Companies should take care to become familiar with the applicable laws, regulations, and standards as well as best practices.

---

### Legal Disclaimer:

*Nothing in this blog is intended to constitute legal advice and your interactions with this blog do not result in the formation of an attorney-client relationship. All matters are different and, as such, nothing in this blog is intended to guarantee, warrant, or predict a specific outcome.*

[Receive E-mail Updates](#)

×

### Receive E-mail Updates

First name \*

Last name

Email address \*

×

Thank you for your message. It has been sent.

×

There was an error trying to send your message. Please try again later.

Submit

Close