



LEVETT ROCKWOOD
P.C.

NEWSLETTER
A Courtesy to Our Clients and Friends

March 2005

TIME FOR A TUNEUP? UPDATING YOUR WEBSITE'S TERMS AND CONDITIONS

Like routine maintenance on your car, periodic review of your website terms and conditions is a good idea. Recent legal developments make it especially important to confirm that your online privacy and other policies are up-to-date.

Disclosure and Content of Privacy Policies

Effective this year, California added some new wrinkles to the longstanding Federal Trade Commission (FTC) guidelines that all websites disclose to visitors whether any personally identifiable information is gathered at the site, and, if so, how that information will be used.

Under California's new Online Privacy Act, any website that gathers personally identifiable information from any California citizen must not only maintain a privacy policy but must also "conspicuously post" that policy on the site. Since the internet has no geographic boundaries, California's law effectively applies to *all* websites that gather personally identifiable information from California residents. Such information includes names, addresses, e-mail addresses, telephone numbers, social security numbers, or any data that would make it possible to contact an individual.

A California-style privacy policy must include, at a minimum, the following five things:

- The categories of personally identifiable information you collect from visitors.
- The categories of third parties to whom you give that information.
- A description of how visitors may review or change their personally identifiable information.
- A description of how you will notify consumers of any material changes to your privacy policy.
- The policy's effective date.

"Conspicuously post" means put a link on your site's home page to your privacy policy. The California law requires that the link contain the word "privacy," and be in a contrasting color to the background, written in capital letters in a font size equal to or greater than the surrounding text.

If you collect any personally identifiable information through your website, you should review your home page and your privacy policy to make sure they comply with the new law as well as with the traditional FTC guidelines. Failure to comply with the California law can lead to civil penalties, and failure to comply with FTC guidelines can be deemed a form of unfair or deceptive business practice.

Sharing Personal Information for Direct Marketing

A second new California law, the Direct Marketing Act, applies if you give personally identifiable information about California consumers to any third party and know (or should know) that the third party will use the information for direct marketing purposes. "Direct marketing" is defined as contacting individuals for the purpose of soliciting their business for profit. The Act is not limited to information collected online; it applies regardless of how or where you collect personally identifiable information.

Fortunately, compliance is easy. All you have to do is clearly and conspicuously provide a cost-free method for people to opt in or opt out of the sharing of their information. If you don't do that, then the Act requires the following specific steps: (1) implement a procedure for California consumers to ask what information you gather and who receives it; (2) give notice that this procedure exists; and (3) respond to inquiries from California consumers within 30 days.

The appropriate method to give notice depends on how you do business in California. If your primary (or sole) contact with California is via the internet, you should post a link entitled “Your Privacy Rights” on your home page. If you have physical locations in California, the Act provides for other methods of notice. Violations of the Act can lead to civil penalties.

Follow Your Own Privacy Policy

Most privacy lawsuits result from the failure of a company to follow its own privacy policy. The problem can sometimes arise from application of a broad “we-won’t-ever-share-your-information” policy in an unexpected context. For example, the FTC sued to stop Toysmart.com from selling its customer list as part of a bankruptcy liquidation. Initially, the FTC appeared to be seeking to block any transfer of the list at all. A compromise eventually was reached allowing transfer to a “family-oriented” buyer of the entire Toysmart.com business, provided that the buyer agreed not to alter the existing privacy policy for any existing customer without an affirmative opt-in from the customer.

To help reduce the risk of unanticipated problems from your own privacy policy, it’s wise to avoid making a sweeping “we-never-share-information” guaranty even if you don’t plan to share information in the ordinary course of your business. At a minimum, you should consider carving out exceptions to allow sharing with affiliated companies, with suppliers necessary to fulfill orders, and with someone buying your business. Failure to do so could result in a rude surprise when you least expect it.

Similarly, you should avoid over-promising security for sensitive information. The FTC recently sued both Petco and Tower Records for not delivering the level of security they advertised. Even if you don’t promise any particular level of security, you still should implement reasonable security measures to protect against unauthorized access by third parties. Liability for negligent security practices is looming on the horizon as a major risk for companies that gather sensitive information.

Protecting Data on Your Site

Many valuable forms of data on your website might not qualify for copyright protection because they are purely factual. Examples may include directories, price lists,

product specifications and the like. Recent court decisions suggest possible alternatives to help stop competitors from using “robots,” “crawlers,” “scrapers,” or other automated devices to harvest non-copyrightable data from your site to compete with you.

The best advice at the moment is to include in your website terms and conditions a provision expressly prohibiting the use of robots or other devices (other than bona fide search engines) to extract data. Such a provision – together with a typical provision prohibiting reproduction of any copyrighted content – may be enforced by the courts and enable you to stop a competitor from engaging in many forms of unfair competition. It won’t stop competitors from manually copying factual data from your site, but it may slow them down.

Recommendations

- Review your website to make sure you have a privacy policy and terms and conditions of use.
- Check your privacy policy for compliance with the new California Online Privacy Act.
- If you give personally identifiable information about Californians to third parties for direct marketing, make sure you comply with the California Direct Marketing Act.
- Allow flexibility to share information when selling your company and in other innocent contexts.
- Ensure that you have implemented at least basic security measures to protect sensitive data, and try to avoid over-promising security.
- Consider updating your online terms and conditions to forbid use of “robots” or other automated data-collection devices.

If you have further questions or would like assistance in reviewing or developing any online policies, please contact **Edward B. Chansky** or **Russell F. Anderson** of our office at 203-222-0885.

echansky@levettrrockwood.com
randerson@levettrrockwood.com
