

Safeguarding Your Business Internet Presence: Part Two, Spotlight on Privacy

By Attorney Patricia F. Claire

This is the second of two articles reviewing basic legal issues of liability avoidance and legal protection applicable to all business Websites.

In the first article, we reviewed what your business as a Website owner can do to identify and protect its rights to the trademarks and copyrighted materials that make up the content of the business Website. The remarkable Internet revolution of the past five years has prompted many companies to assemble their intellectual property portfolio for the first time, and to take appropriate steps to protect these valuable assets. We reviewed the fundamental legal principles of intellectual property ownership and contract law that continue to apply in the on-line context. This second article will examine another current hot issue in Internet law, arising from legal relationships with users of a business Website. The issue is on-line privacy protection.

Concerns about on-line privacy have been receiving a great deal of attention in the popular and industry press, as the spotlight is turned on the unprecedented opportunities that exist for undisclosed on-line surveillance, profiling, sale, and use of personally identifiable information. Government agencies flooded with complaints have begun to investigate Websites and to take legal action against privacy violators. What steps should every business be taking with regard to privacy considerations of the users of its Website?

Relationships with Website Users

A business Website may be what is now characterized as a “traditional” commercial Website, essentially providing a retail catalog and on-line purchasing opportunities. But even if a Website is not a retail sales site, every business Website has some relationship with its users. The site may provide a brochure of information about the goods or services of the business, a means of pursuing employment opportunities at the business, a portal to other Websites, a means of participating in an on-line vertical marketplace, or general information on topics related to the field in which the business operates. The desired users may be other businesses: suppliers, purchasers, retailers, distributors, franchisees, or other affiliates. Desired users may be individuals such as potential employees, subscribers or consumers of goods or services purchased by means other than on-line.

A business may use its Website, in any of these capacities, as a means of collecting information about its users. Or because of relationships with Web-based companies such as advertising brokers, the Website of a business may serve as a tool for third parties to collect information about the users. The collection of information about users by and through business Websites is a cause of rapidly growing concern not only among individuals but increasingly, within the state and Federal governments.

Which laws govern on-line privacy

With a few exceptions, the development of privacy policies for Websites has been a voluntary effort, like so much Internet activity. Contrary to general belief, there is no Constitutional right to privacy in the United States, although cases have been decided that have established certain limited rights with regard to personal privacy. Privacy of personal information is an evolving area of the law, accelerated by the growth of the Internet. Although new legislation has not yet been enacted to regulate the privacy practices of all business Websites, there are three specific areas where Federal laws already exist that directly address information privacy. These are the Children's On-line Privacy Protection Act (COPPA), effective for over a year; the Financial Institutions Modernization Act (commonly known as the Gramm-Leach-Bliley Act), fully effective July 1, 2001; and the personal health information protection provided under the Health Insurance Portability and Accountability Act (HIPAA) implemented in 2003. Another area concerns doing business within the European Union, which has enacted a far-reaching Privacy Directive that is the subject of an E.U.-U.S. safe harbor agreement. By now a company operating within the purview of any of these laws should have designed, and if relevant have implemented, a plan for timely compliance.

COPPA established a first step in direct regulation of a broad range of business Websites. The Federal Trade Commission (FTC) already has begun to take enforcement action under COPPA against Websites that, in violation of the law, collect personally identifiable information from children under age 13 without posting a privacy policy and without prior parental consent.

In addition to COPPA enforcement, the FTC has been observing and then reviewing the unregulated, voluntary efforts of businesses to establish privacy practices and state their policies on their Websites. So have the Attorney General offices of various states. The FTC has published guidelines for appropriate privacy policies, but its surveys have led to the finding that voluntary compliance is not producing adequate disclosure and fair privacy practices. As a result, the FTC has recommended to Congress the enactment of legislation requiring compliance with these standards.

In the absence of new legislation specifically targeting the Internet, Federal and state agencies alike have begun to make use of existing laws to prevent unfair and deceptive trade practices in the operation of Websites. The office of the Michigan Attorney General has become

very active in this area, taking action under the Michigan Consumer Protection Act against business Websites that fail to disclose, or that misrepresent, their privacy policies.

What is needed in a Website privacy policy

In conducting a business Website legal audit, we proceed page by page through the Website. Some businesses are surprised to find how extensively which their Website has been set up to collect information about the users. Other businesses are aware of their own information gathering and use practices, but may not fully understand arrangements they have made for third party collection of information - especially the ultimate uses intended to be made of that information. Lack of knowledge about information collection practices can lead to legal problems for the Website owner, which is responsible for the accuracy of the privacy policy stated on the Website as reflected in actual practices.

Most simply stated, at a minimum a business needs to know and accurately disclose what information is being collected through its Website, and for each type of information: by what entity is the information collected, where it is stored, for how long, how it is used, are cookies or Web bugs placed by the business Website and/or by third parties, is information shared, with what entities, for what purposes, is it combined with information from other sources, can users choose whether or not to provide the information, can users review their information, can they modify their choices, what security exists to protect user information, and how are changes in the policy handled. Information collected includes not only “visible” information voluntarily provided by a user for such apparent purposes as registration for access passwords, requests for information and customer service, responses to surveys and contests, and order and subscription forms. It includes “invisible” information collected such as the IP address, the domain from which the user reached the Website, the type of browser used, and the pattern of travel among the pages of the Website. The business is responsible for seeing to it that the policy stated on the Website reflects the actual operations of the business and discloses third party involvement.

Because so many Websites already have privacy policies presented on-line, there is a tendency to simply copy the written policy of another, comparable site. This rarely will result in a company’s actual information privacy practices being expressed in its written policy, yet accurate expression is a key to avoiding complaints of unfair and deceptive trade practices. And, as practices and technology change, a privacy policy needs to be kept up to date, while recognizing that individuals relying on having provided information under an earlier policy may want to opt-out when the policy changes. Finally, the privacy policy should be easy to find on the Website, located not only on the homepage but wherever visible information is collected about users.

Often the process of creating a written privacy policy for its business Website prompts a company to assess its information privacy practices and its relationships with third party collectors of information about its users. Attempting to meet the basic, voluntary FTC standards can have the positive effect of a company defining the business purposes for which it is collecting, using and retaining user information through its Website. Businesses that go through this process, minimize the information they collect and clearly state and adhere to their Website privacy policy may find this helps to avoid liability, enhance their reputation and provide a competitive edge as the privacy debate continues to heat up.

Patricia F. Claire is an attorney with Willingham & Côté, P.C. in East Lansing, Michigan, and heads the firm's Intellectual Property, Internet and E-Business Law Group. She can be reached at pclaire@willinghamcote.com or (517)351-6200.