# The Internet: By All Means, Use It, But Use It With Caution

May 4, 2012

Everyone not living under a rock now understands that an Internet presence is vitally important to almost every kind of business, but not everyone understands the associated legal risks. A business's use of the Internet presents not only increased exposure to some of the risks it would face in a paper-and-ink world, but also new risks that are specific to cyberspace. This article addresses a few of the legal issues involving the Internet and email that many businesses overlook.

**Website Privacy: A Growing Risk**

During the past year, Facebook®, Twitter®, and Google® each have settled disputes with the Federal Trade Commission ("FTC") relating to website privacy. Class action lawsuits have been brought based on similar claims, and a recent suit reportedly settled for several million dollars. Even though national and international businesses capture the media headlines, privacy policies are not just for large companies or "Internet-based companies." Almost all businesses with websites collect information from people in some way and, therefore, are advised to establish, post, and comply with website privacy policies and terms of use to protect them from liability. Websites that facilitate transactions may trigger additional obligations and, if credit is extended for online transactions, the number of applicable laws – and the corresponding compliance burdens – increases significantly.

**Don't Promise the Moon**

In the area of website privacy, one of the most frequent violations of the law and source of liability occurs when businesses make assurances in their website privacy statements that they fail to honor in practice. This shortcoming is considered by the FTC to be an "unfair and deceptive trade practice," and allegations of this sort can be found in many of the FTC's recent enforcement actions in this area. This is particularly unfortunate when a business has inadvertently created an avoidable risk by establishing privacy standards that are stricter than those required by law. This problem most often arises when a business (or its third-party website designer) simply mimics a privacy policy statement found online or uses a "do-it-yourself" document service without carefully tailoring the policy to the company's specific industry, location, and practices. A policy required for a medical practice in California may be far beyond that required for a retailer in North Carolina.

**Caution! Children at Play**

Websites directed at children, whether in whole or in part, are subject to additional restrictions and requirements under the Children's Online Privacy Protection Act ("COPPA"). If a website has a section directed at children, specific disclosures and policies must comply with the COPPA rules which include limitations on third-party sharing and parental consent, review, and control requirements.

A number of factors are used to determine whether a website is directed at children, such as whether its subject matter and language are child-oriented, whether it uses animated characters, and even whether advertising on the site (which may come from third parties) is directed at children. Even if a website is not directed at children, it has become customary to include COPPA language in a privacy policy or terms of use to protect the business and remove any ambiguity that may exist.

**Location, Location, Location**

A few states have their own website privacy rules, some of which apply generally and others specifically to the online arena. California's privacy laws are widely regarded as the most rigorous. California's Constitution recognizes an "inalienable right" to privacy, and California's privacy laws are policed by a dedicated state agency – the Office of Privacy Protection. If a company's website or email marketing is directed at California residents (including efforts directed at national audiences generally), the company will need to comply with California's very specific privacy requirements. California law regulates, for example, the font size and color of a required link from a website's home page to its privacy policy statement.

**Online Advertising and "CAN-SPAM"**

Companies may collect information through their websites, or in other ways, for the purpose of marketing products and services through email or other electronic messages. These companies sometimes neglect the requirements applicable to electronic advertising messages. The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (commonly known as the "CAN-SPAM Act") requires those advertisers, among other things, to "clearly and conspicuously" identify every commercial electronic message as an advertisement, provide the physical address of the sender, and include an opt-out mechanism to allow recipients to avoid future communications. Requests to opt out must be honored within ten days, and there are specific limitations on the opt-out mechanisms that may be used. For example, a telephone number, even if toll-free, is not an acceptable opt-out mechanism.

In addition, the CAN-SPAM Act prohibits the use of misleading information in the header fields of a message. For example, an advertising email message with the subject "You've Won!" is probably in violation of the CAN-SPAM Act if the recipient has not actually won anything. Similarly, if the name displayed in the "from" field does not correctly identify the sender, there is likely a violation.

The CAN-SPAM Act limitations do not apply to communications relating to a transaction or relationship that has already begun. For example, an email that merely confirms payment for a transaction previously initiated is not required to include CAN-SPAM Act disclosures. In many cases, companies attempting in good faith to differentiate between advertisements and transactional or relationship communications struggle to do so, particularly with regard to messages containing both categories of communication. For this reason, some companies are advised to include CAN-SPAM Act disclosures in all email messages to avoid the risk of inadvertent violation.

More businesses are entering the social media arena every day to take advantage of the marketing potential it offers. They are well-advised to remember the CAN-SPAM Act when crafting innovative social media marketing strategies. Courts have recently ruled that the CAN-SPAM Act, which was written before social media became prominent to address widespread abuse of the then new concept of email advertising, nevertheless applies to social media messages.

In addition, many social media companies require users to agree to terms of use or similar contracts that may prohibit or restrict advertising practices. Facebook® and MySpace® each have sued commercial users under the CAN-SPAM Act for misleading advertising practices that violated the social networks' respective terms of use. Because the nature of social media platforms is usually more complex than email, CAN-SPAM Act compliance issues can be more complex as well; an advertiser's responsibilities are less clear the more a social media platform differs from traditional email. For example, if a social media platform limits the number of characters that can be used in a message, how does that affect the sender's compliance obligations? As in many areas, the law is struggling to keep pace with technology and social phenomena.

It has become customary, although not required, to address the CAN-SPAM Act in a business's website privacy policy statement or terms of use by including a link to an opt-out mechanism. Although website privacy and opt-out are legally separate issues, users have come to expect to find both kinds of information in the same location. Integrating disclosures may also help to avoid confusion as to which statement applies in some cases.

Businesses are advised to give careful attention to CAN-SPAM Act compliance before sending electronic advertising messages. Failure to observe the requirements of the CAN-SPAM Act can result in penalties of up to $16,000 per violation,

as well as criminal prosecution.

**Conclusion**

Violations of the various laws and policies regulating commercial websites and email are gaining increasing attention from governmental entities, consumer advocacy groups, and plaintiffs' class action attorneys, and are expected to be an emerging source of risk for many businesses.  Fortunately, much of that risk is avoidable if care is taken to learn the patchwork of applicable legal requirements, adopt appropriate policies, and enforce those policies consistently.

--