

# COX SMITH MATTHEWS

## Commercial Email, Website and Technology Agreements, and Cyber-Insurance

by Bart Huffman, Brett Schouest and Meagan Gillette<sup>1</sup>

### *Commercial Email*

Commercial email is regulated by CAN-SPAM<sup>2</sup>, the federal legislation which also provides penalties for those who spam and companies whose products are advertised in spam. CAN-SPAM divides the universe of email messages into two categories – commercial email and transactional or relationship email. Commercial email is that which promotes commercial products or services, while transactional/relationship email is that which facilitates a transaction or otherwise communicates with a customer concerning an existing business relationship. CAN-SPAM's requirements are directed to the commercial email category

The statute's requirements are designed to ensure that a recipient can recognize an advertisement as such, to help minimize deception, and to provide a recipient the ability to opt-out of receiving commercial messages from the sender in the future. If the sender has not obtained the recipient's prior affirmative consent to receive the message, a commercial email message must contain clear and conspicuous notice that the message is an advertisement or solicitation. The most common way to obtain affirmative consent (and thereby avoid the "solicitation/advertisement" label requirement) is to provide an Internet user with a dedicated opt-in "click" box clearly reflecting the user's consent to be included on one or more email lists.

The requirements of CAN-SPAM should not be taken lightly. The federal legislation provides several enforcement mechanisms, including civil actions by state attorneys general and Internet service providers, as well as the possibility of criminal prosecution.

### *Website Agreements*

Commercial transactions on the Internet differ in some respects from transactions that occur on paper. When constructing the terms of the agreements that will govern the parties' relationship, it is important to remember that website users and customers are typically not represented by attorneys. Accordingly, while the operator of a website (and its attorney) has substantial freedom in crafting a website agreement, a rule of reason will bear heavily on the enforceability of the chosen terms.

When constructing an online agreement, the first step is a solid understanding of the data involved. Different types of data – submitted data (*e.g.*, names, email address), generated data (*e.g.*, reports, purchasing history), or user content (*e.g.*, pictures, video, essays, music) – will raise different concerns and require different approaches. In addition, an operator should always aim to manage the users' expectations. Non-deceptive communication of terms, conditions, intended use, and other policies can go a long way in protecting the operator from subsequent criticism and liability.

---

<sup>1</sup> Messrs. Huffman and Schouest are shareholders with the law firm Cox Smith Matthews Incorporated. Mr. Huffman's practice is focused on Internet and other intellectual property matters, and Mr. Schouest's practice is focused on business litigation and insurance coverage issues. Ms. Gillette is an associate in the firm's Intellectual Property section.

<sup>2</sup> Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037 (2006).

# COX SMITH MATTHEWS

While many provisions of website agreements are typical of consumer contracts, the website context generates a number of nuances. For example, website operators may want to carefully consider and craft provisions governing termination rights, targeted advertising, the ability to assign/transition business and data (*e.g.*, when companies and websites are bought and sold), indemnification rights (especially when users upload or manage content), and security concerns. Somewhat challenging topics, which call for more creative approaches in the Internet context, are liability limits, choice of forum and governing law, and alternative dispute resolution provisions.

## *Internet Technology Agreements*

Often, the approach of the Internet technology provider is similar to that of a pure software licensor – the provider seeks to disclaim all responsibility and to place all responsibility on the purchaser or Internet business partner. The technology “purchaser” will, on the other hand, often view the Internet technology provider similar to other service providers, believing the Internet technology provider should accept full responsibility (including representations, warranties, and indemnification and insurance obligations). It is easier (and far less costly in attorneys’ fees) if the business representatives negotiate on a somewhat more detailed basis when they are in the process of deciding whether to pursue the “deal.” The attorneys should be able to assist by providing a checklist of terms to be worked out, to the extent possible, in advance.

## *Insurance Issues*

Just like many other methods of conducting business, e-commerce services and transactions involve significant issues and risks. Like all other business functions, it is important to insure against such risks where possible. Relatively new products are offered in the insurance market, referred to as “cyberinsurance,” which are designed to bridge gaps between traditional insurance coverages and those needed for e-commerce transactions. First-party or “cyberproperty” coverages include data theft/destruction and rehabilitation, extortion/“cyber-ransom”, e-theft/e-fraud (unauthorized e-transactions) and business interruption/denial of service. Third-party or “cyberliability” coverages include libel/slander/defamation and trademark/copyright infringement liability associated with websites and emails, hyperlinking liability (passing computer viruses), contextual liability (professional services over Internet), network security breaches and denial of service liabilities.

One size does not fit all and, like other insurance risks, it is important to consider your business model for risks to cover. Assessment of security of your current computer system and programs, as well your current insurance coverages, is important in identifying and obtaining the right cyberinsurance for your needs. Insurers offering cyberinsurance provide questionnaires and application documents to guide you through such assessments. At this point, cyberinsurance remains largely untested in the market and courts, but it is becoming increasingly popular and necessary as doing business through e-commerce continues to take hold in the American and world-wide economy.