ECOMWORLD
www.ecomworld.com

Minimizing the Legal Risks of Electronic Commerce
by Lawrence Savell
Article published 06/21/01 on Ecomworld.com

Companies contemplating and undertaking e-commerce and other Internet business efforts need to be sensitive to—and be prepared to deal with—a wide range of potential legal liabilities.

They range from dealing with an array of laws and regulations that often vary from country to country and state to state, to insuring that the privacy of online users is respected.

As the Internet is an international medium, companies operating Web sites or participating in e-commerce ventures may be subject to the jurisdiction and laws of courts around the world. In disputes among parties located in different countries, key issues are where can you be sued and whose law applies. The result can significantly impact defense costs and convenience, and maybe even the outcome.

The question of where can you be sued basically asks under what circumstances can the maintenance of a Web site expose a company to a lawsuit in a particular jurisdiction. One answer is provided by the "Brussels Regulation," an European Union rule that will go into effect in March 2002. It allows European online users to sue, in their own courts, online sellers that have EU branches, regardless of where the seller is actually based. < /P>

Another European initiative, the so-called "Rome II," is the European Commission's proposed law governing cross-border Internet commerce. It covers such matters as defamation, unfair competition, marketing and consumer protection, and takes a different approach from prior pronouncements.

Many other European regulations look to the law of the country where the supplier or Web site is situated— the "country of origin" principle. By contrast, Rome II looks to the law of the buyer's country.

Suppliers are concerned that adoption of Rome II will create inconsistencies and uncertainty, and place a huge burden on those selling on the Internet to keep track of applicable laws, hampering e-commerce. Buyers favor the change, and the comfort of familiar local laws, and claim this will foster e-commerce.

In addition, a new Hague Convention—a treaty to be adopted in June by a conference of 48 nations—states that an online business could be liable under the laws of any of the member countries. The treaty would allow customers to sue businesses in the courts of the country where the customer lives. It also allows for enforcement of foreign judgments in such matters as intellectual property claims, contractual disputes and libel.

In the United States, meanwhile, a Web site operator that conducts business could face a suit outside of the company's home state. Sites that are "passive" and merely informational will probably not be subject to out-of- state jurisdiction.

Digital Signatures

Last year, President Clinton used a smart card and his dog's name as a password to sign the Electronic Signatures in Global and National Commerce Act, which became effective Oct. 1. The law specifies that any electronically transmitted signature is to be considered as legally binding as an actual written, paper-based signature. It overcomes many of the inconsistencies in state laws on this issue.

Included are digital signatures, digital code that can be attached to an electronically transmitted message and uniquely identifies the sender.

The statute, however, does not define in detail what constitutes a legitimate, safe and secure digital signature. It may be an electronic sound, symbol or process attached to, or logically associated with, a contract or other record, and executed or adopted by a person with the intent to sign the record.

Presumably, a reply e-mail could satisfy the requirements of this definition. The problem is that the requisite "intent" will likely be difficult to decipher and might be the basis for future litigation.

The act does not require any person to agree to use or accept electronic records or signatures. It declares the validity of electronic signatures for interstate and international commerce. But the act is a federal law, thus it only applies to a contract or record involving interstate or foreign commerce. And there is no guarantee that electronic signatures will be recognized outside the United States.

Several U.S. states, meanwhile, have their own e-signature laws, including California, Illinois, and Utah.

In addition, other countries have e-sign initiatives, including Germany, the United Kingdom and Ireland. There also is an EU Electronic Signatures Directive which stipulates that an electronic signature cannot be legally discriminated against solely on the grounds that it is in electronic form, and that if certain requirements are met, there will be an automatic assumption that the electronic signature is as legally valid as a hand-written signature and can be used as evidence in legal proceedings.

But even with such official recognition, it still is important for e-commerce companies to maintain a time- stamped file copy of any electronic final agreement in a tamper-proof and secure manner to protect against deliberate or inadvertent alteration of the contents.

In addition to the issues that can arise when parties from different countries and states conduct business, e- commerce participants also need to be aware of the legal implications from operating Web sites. Company should make sure that they have the right to use the text or illustrations that appear on their sites.

The use of material to which another owns the copyright may provide the basis for an infringement claim. Parties must be cautious in assuring that posted text and pictures are either internally created or commissioned by the Web site operator as a "work made for hire," or that permission has been obtained from the copyright owner.

Other sources of potential liability are "framing," in which a company displays part of another Web site in a window on its site, and linking to specific sub-pages of another site

without permission. The law on these matters—represent a conflict between protection of intellectual property and freedom of online speech—is unclear. Court rulings on the matter are inconsistent.

A plaintiff may allege that a company's link to another's Web site makes the company responsible for the content of that other site. To minimize the risk of such a claim, links to third-party sites should be accompanied with a notice disclaiming responsibility for, and affirmatively denying any endorsement of, products, services or information contained on that outside site.

Defamation and Libel

E-businesses also must guard against posting information on their sites that can defame a person, entity or product. Such a situation can provide the basis for a libel or disparagement claim.

While definitions vary, the key is injury to reputation. Traditional classifications of libelous words include those claiming incompetence in trade, occupation, office or profession, or questioning a corporation's integrity, credit or ability to carry on business.

Many Web site operators have posted privacy guidelines, promising to protect the confidentiality of user information that may be provided or collected. If such promises are made, they must then be kept.

Privacy is becoming an important issue around the globe. An EU directive forbids the collection of data without the consent of individuals. Similar legislation has been enacted in Canada—where authorities state that the goal is to bolster consumer confidence in e-commerce— and Australia and India.

The use of disclaimers and qualifying language on Web sites can reduce exposure by affirming that no warranties are being made and denying any liability for damages. Specification of the other terms and conditions under which the site and its information are being made available, coupled with a "click-through" agreement from users before proceeding further onto the site, may provide some additional legal insulation.

Firms also should determine if their activities are covered by existing insurance policies or if additional coverage is required for business interruption issues or Web-based fraud.

Online businesses should follow the operating rules that are common in the offline world. But because the benefits of technology may present new pitfalls, it pays to keep the legal considerations in mind. It often is helpful to avoid situations where the potential liability is greatest, and to keep legal counsel informed and involved at all stages of the process to reduce potential exposure.

Lawrence Savell
Lawrence Savell is an attorney concentrating on litigation defense and counseling in the New York office of Chadbourne & Parke LLP.