Online Law

Chapter 12

The Rules of Doing Business Online

Mike and Kathy own a small retail business. They wanted to expand their business by selling online, so they hired a company to procure a domain name and design their Web site, complete with an online catalog and a shopping cart.

The Web site worked fine and their sales, while not spectacular, did expand beyond their local community. They were getting orders from customers throughout the United States and several foreign countries.

Then the surprises started. When the domain name was up for renewal, they received a substantial invoice from the Web site design company as well. “Hey, I already paid you,” Kathy told them. “Yes, you did,” they replied. “But we own the copyright to your Web site, so if you want to continue using it, you’ll need to pay us the annual license fee.” Kathy was not impressed. “Well, we’ll just take our business elsewhere,” she said. “Go ahead,” they replied. “But we own your domain name, so you can’t move that, and you need to understand that you can’t use anything from your existing Web site on some other site. If you do, that would be copyright infringement and we would sue you.” Rather than start again from zero, Mike and Kathy ended up paying this company again and again for the work they thought they had already paid for.

The next surprise was when they started receiving return shipments of expensive electronic equipment they had sold to some customers in Europe several months previously. All the equipment was heavily used and not in good condition. They e-mailed the buyers, stating that their company policy was “no returns after 30 days.” They received a response from an attorney who said, “Your policy is not enforceable; European law applies and, because you did not provide the required legal notices, my clients have an absolute right to a refund.” The credit card company had already charged back the amounts, and after checking with their lawyer, Mike and Kathy realized there was nothing they could do.

The final surprise was that, when they typed the name of their company into various search engines, the first thing that kept popping up was the name of a competitor. They soon discovered that the competitor was far more successful at selling online, using Mike and Kathy’s company name. No wonder their online sales were sluggish!

Such stories are not hypothetical situations; they happen repeatedly.

Doing business in cyberspace means being subject to a somewhat different legal environment from doing business at a physical location. Some examples:

- **Web-related service contracts.** It is important to pay attention to copyright and ownership rights. Unless there is a written agreement to the contrary, whoever designs your company’s Web site owns the copyright to it. Also, make sure the designer doesn’t copy from some other Web site, leaving you with a potential infringement suit.
- **Contracts without signatures.** A written signature is no longer required to form a contract; a click on a Web site button that says “agree” is enough. It is important that every online transaction be treated as a real contract, with adequate terms and conditions, limitations on liability, etc.

- **Applicable law.** If you are selling consumer goods, there are restrictions on how much you may limit your liability, and you may not be able to specify that the law of your own state applies.
- **Privacy law.** Both as a legal and as a practical matter, it is important to implement and post a privacy policy that complies with the law in the buyer's jurisdiction.
- **E-mail solicitation.** The federal CAN-SPAM Act governs commercial solicitations via e-mail. It is easy to comply with, but compliance is mandatory and the penalties for noncompliance can be substantial.
- **Minors.** There are strict limits regarding correspondence with, and collecting information about, anyone who is or is likely to be a minor. Any online seller of goods or services targeted at minors needs to be aware of the numerous laws protecting minors in an online environment.
- **Export regulations.** Most goods can be shipped overseas without special licensing or permits, but certain software and high-technology goods are restricted.
- **Trademark law.** Putting the name of your business and products online exposes them to the world. You need to be sure your marks do not infringe anyone else's marks, and you need to protect them from infringement by others.
- **Search engine optimization.** While not solely a legal issue, optimization involves using specific words and phrases in a Web site, often as *tags* to enable the search engines to find your Web site. Such tags, often called *keywords* or *adwords*, can be purchased from search engine companies so that, when a user types in that particular word, the search results will include a link to the Web site of the company that bought the word. Company names, trademark names, and the names of a particular type of product are often used as keywords, etc. There have been lots of lawsuits involving companies that purchase competitors' names as keywords, thus diverting traffic perhaps intended for a competitor's site. It is important to consider such issues when implementing a Web site.
- **Advertising.** More and more jurisdictions are enacting laws restricting the use of e-mail for advertising purposes, even with respect to existing customers. Before sending out anything that could be construed as advertising, be sure you're legal.

These are just some of the issues that need to be considered. There is certainly no reason to shy away from doing business online, but prevention of problems is always better than having to solve them.

–by Robert L. Ellis, Columbus attorney and former chair of the OSBA Digital Technology Law Committee; rellis@petersonellis.com.

Use Your Trademarks Wisely and They'll Serve You Well

Your company's trademarks are valuable assets which, with proper treatment and due care, can serve you well for many years. The U.S. Patent and Trademark Office defines a trademark as a word, phrase, symbol, design, or combination of these, which identifies and distinguishes the source of the goods or services of one party from those of others. However, many trademarks, which were once proud possessions of large corporations, have been lost through misuse or because they became generic. "Aspirin" and "cellophane" are examples of marks that are now generic terms and no longer identify any particular company's product. If your company's trademarks were lost, they could be used by anyone and would no longer signal the public that the products and services they stand for are from your company. It is relatively easy to protect and care for trademarks. Follow these simple rules in all uses of your trademark, wherever it appears:

1) **Use trademarks in a distinctive manner.** Always distinguish your mark from the surrounding text. The general rule is to capitalize trademarks completely, put them in italics, use initial caps with quotes, or, at a minimum, use initial caps. If you have a stylized word for a mark, consider using the stylized depiction even in text. Whatever depiction you choose for the mark should be applied consistently.

2) **Identify trademarks with their status.** If a mark has been registered in the United States Patent and Trademark Office, "®" should be used with it. If the mark has not been registered, "TM" should be used. If it is an unregistered mark for services rather than goods, it should be marked with "SM." At the least, the proper status identifier should be used on all prominent appearances of the mark and on the first appearance of the mark in any text.

3) **Trademarks are proper adjectives. Use them with the generic name of their product or service.** At a minimum, use the generic term after the trademark at least once in each document, preferably the first time the mark appears. For example, "Windows XP® operating system is the preferred operating system for corporate IT departments," or, "The RegulatorPro™ UPS takes power management even further."

4) **Never use trademarks in the possessive form.** Trademarks should never be used in the "…'s" form, unless the mark itself is possessive such as "McDonald's® restaurants."

5) **Do not pluralize your trademark.** Since trademarks are not nouns, they should never be used in the plural form. Instead, pluralize the nouns they describe. For example, use "ThinkPad notebook computers are superior" rather than "ThinkPads are superior."

6) **Trademarks are never verbs.** For example, write "Xerox® photocopiers allow you to photocopy documents the way you want," NOT, "You can Xerox® any document the way you want."

7) **Trademarks are privately owned; always indicate the owner.** You can indicate the owner's name with a simple footnote or notice paragraph that could appear on the cover page, the copyright notice page, the bottom of the page on which the trademark is used, or on the last page. For software, the owner's name can appear on the log-on screen, the splash screen, the "About" screen, or another similar place. The notice may read, for example, as follows: "The following are trademarks or registered trademarks of Microsoft Corporation: ActiveX, PowerPoint, XL and design (the Microsoft Excel

logo).” You may list marks in their stylized or design form, or in descriptive form as the Microsoft Excel logo was listed in the sample notice above.

–by Alan J. Hartman, a partner in the Cincinnati firm of Dressman Benzinger LaVelle psc.

Be Careful When Using Internet Services

Many business owners and entrepreneurs learn the hard way that the Internet is a mixed bag of unpredictable services: some sources of information are reliable, and some are not.

I recently was informed about a couple of new business owners who decided to start a company. They turned to the Internet for help incorporating their business. They found a company—let's call it ABC Incorporations.com—that promised to set up their corporation for less than an attorney would cost. ABC Inc.com did not help them decide if they should be incorporated or discuss with them relative benefits of establishing an LLC versus a corporation or other business entity. The new entrepreneurs did not know to ask these questions. They simply filled in the online form and sent in their application.

A few weeks later they received their certificate of incorporation from the state of Ohio and a host of other materials regarding the company set up by ABC Inc.com. The company had made its representative the owner of the business and a local individual at a mailbox store the statutory agent. The business owners who had paid the Internet company to set up their corporation basically had transferred the ownership of their business to the Internet company.

I do not know whether the Internet company intentionally made itself the owner or simply made an error, but I doubt the new entrepreneurs had intended to transfer their business to an out-of-state party.

What this example points out is the significant risk you take when dealing with nameless, faceless Internet providers. When you use the Internet for business, keep these tips in mind:

1) Know whom you are contacting and whether or not they have a physical address. It can be very difficult to get problems resolved if you cannot even find the people who run the Web site.
2) Make sure the company has the experience and credentials to do the job. Remember, almost anyone can create a professional-looking Web site.
3) Google them. One of the best ways to learn about a Web-based company is to use an Internet search engine to see if there are any articles or information available from third parties about the site.
4) Take a test drive. Give an Internet company a small project and see how your account is serviced before committing to a significant amount of business or service.
5) Send them an e-mail. Many Web sites publish e-mail addresses, but never respond to e-mails. E-mail a Web site provider seeking more information before working with a site. If a company cannot respond to you before you buy, how likely is it that you will get a response after you have given your money and there is a problem?
6) Think about what you send out. Do not send proprietary, financial, or other sensitive information to a Web site you do not know or trust. It is not enough to be notified that the Web page is secure. If you must send particularly sensitive information, ask for a mailing address and send it by certified mail so you can limit the accessibility of the information and will have a physical address should something go wrong.

The Internet can be and is used successfully for business and legal work. By using the above tips and strategies you will be better able to avoid Internet problems and the pitfalls associated with Web businesses.

–by Jeffrey J. Fanger, the managing member of the Cleveland law firm of Fanger & Adelman LLC.

Cyberlaw: How To Manage Employee Access to the Internet

Q: I own a small business and am planning to give only one or two of my employees Internet access. Is there anything I should do to protect the business from employee use of the Internet?

A: While the Internet is clearly a great business tool, any business—small, or otherwise—that makes the Internet available to employees should consider the impact of that decision on productivity and on potential liability of the business for an employee's use of the Internet. "Surfing the 'Net," downloading pornography, and sending offensive e-mails are the types of incidents employers report. Limiting Internet access to only those employees who can use it for business purposes helps limit these concerns. You have no obligation under law to provide access to the Internet to all of your employees. Courts have treated the Internet as just another tool provided to an employee to perform his/her job duties. It may be wise, however, to prevent access by unauthorized personnel by keeping the work station used for Internet access secure or providing Internet access using password-only access. You should make clear to users exactly what is permitted use of the access. You should develop a written Internet use policy that the employee signs, including a statement that he or she has read and understands the policy and agrees to abide by it. You should discuss this policy with your labor attorneys to ensure that the policy's application does not transgress existing labor law or violate other company policy.

Q: What should be included in an Internet use policy?

A: Many policies state that the workstation and Internet access are the property of the employer and are provided for the employee's use in fulfilling his or her job responsibilities. Ideally, Internet access will be supported by the employee's written job description. Employers should make clear that the Internet is insecure, so that privacy of Internet communications cannot be guaranteed, but that the company also reserves the right to monitor employee Internet access to identify any who misuse their access. Employers should consult with their attorneys regarding the law relating to monitoring of employee communications.

Q: Should the policy contain other rules to protect the company and its employees from violations of the law?

A: Generally, in addition to addressing the matters suggested above, an Internet use policy should:

1) discourage employees from downloading information from the Internet in order to avoid such problems as copyright violations and printer congestion;
2) prohibit employees from visiting or downloading sites that are unrelated to their job requirements, especially pornographic sites;
3) include prohibitions against sending e-mail messages, including jokes, that are offensive generally, or include racial, sexual, or gender-related slurs, or defamatory remarks;
4) prohibit Internet use for commercial transactions, including unlawful sales of drugs or sales of cigarettes or alcoholic beverages to minors, or employees' purchase of goods, whether employment-related or not;
5) prohibit employees' use of the Internet to discredit the employer's reputation or that of a colleague, or to disclose sensitive company information, such as trade secrets or personnel matters;

6) prohibit the use of e-mails as a substitute for formal business letters (the informality of e-mails and the fact that e-mails are easily forwarded to unintended recipients can create litigation or complicate its defense).

–by Mary W. Christensen and Timothy J. Owens, partners in the law firm of Christensen Christensen Donchatz Kettlewell & Owens LLP.

Electronic Signatures: Might You Sign a Contract Without Realizing It?

It is no longer necessary for you to physically place your signature on a piece of paper in order to enter into a contract. Instead, simply replying to an e-mail can mean entering into a valid and binding contract to buy insurance, sign a lease, arrange for utility service, or take out a loan. Chances are you have already signed agreements electronically by clicking the "I agree" buttons on various Web sites. The electronic signature era has arrived.

As e-mail and other forms of electronic information exchange became routine, there were many attempts to define an electronic equivalent for a person's physical signature on paper. In the 1990s, the concept of *electronic signature* was introduced to try to legitimize contracts that were not physically signed. The focus back then was on encryption, which would make electronic signatures "forgery-proof." International organizations proposed, and some countries passed, laws specifying detailed standards for electronic signatures, most of which were ignored as businesses simply exchanged e-mails.

Since then, practical considerations have prevailed. In an electronic context, the risk of forgery is not greater than in a paper contest, and neither encryption nor detailed standards for electronic signatures has been useful. The current electronic-signature laws in effect at both the state and federal level are much broader and more practical. The federal version is the Electronic Signatures In Global and National Commerce Act (E-SIGN). E-SIGN is significant because it means that electronic signatures will be valid for commercial transactions throughout the United States and for all international commercial transactions based on United States law. Although E-SIGN does not mandate the use of electronic signatures, it does mandate their validity. It specifically invalidates state laws requiring paper signatures, as well as state-level electronic signature laws and court decisions that have conflicting provisions. It also permits businesses to require electronic signatures of their customers as a condition of doing business. Also, many laws that used to require retention of paper originals have been pre-empted, and it is now permissible to retain copies of many types of documents in electronic rather than paper form.

Q: What is an "electronic signature"?

A: E-SIGN deliberately avoids imposing any specific standards, and instead defines it broadly: "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." This definition means that a faxed signature on a contract is as good as an original, but the law goes far beyond that. The concept of a signature as being limited to a physical mark on a piece of paper has been abandoned. In its place is the concept of *electronic indication of assent*. Contracts can now be entered into by pressing "1" on a phone, by entering a pin number, by clicking a box on a Web page, or—if the privacy aspects can be ironed out—even by means of a biometric identifier (a biometric identifier might read, "Please sign the rental agreement by placing your thumb on the ID pad"). An oral statement or a recording of an oral statement is specifically excluded, so when you are signing a contract via your phone, you won't hear the phrase, "Press or say 1." You'll just hear, "Press 1."

Q: What about contracts that must be notarized?

A: E-SIGN also permits electronic notarization. This raises some intriguing questions: Since people now can do major transactions at home after hours (not only at real estate offices and banks during working hours), and since notaries still have to personally witness the person signing the contract—even if both the person signing and the notary use electronic signatures—will every pizza delivery person and cab driver become a notary public?

Q: Is it possible for computers to make contracts without involving people?

A: Yes. Even more intriguing for businesses is the provision in the law that allows contracts to be formed by *electronic agents*. *Electronic agent* is defined as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response." Thus, binding contracts can be formed by machines, without the direct participation of any human being. Although this sounds revolutionary, the law is merely enabling on a broad scale a practice known as Electronic Data Interchange (EDI). EDI has been used for many years to accomplish such things as automatic inventory replenishment. Before E-SIGN went into effect, EDI had to be the subject of prior agreements between individual companies. Now any company can, in effect, offer EDI without any prior agreement.

Q: Is there any type of contract that cannot be signed electronically?

A: Yes. E-SIGN does have some limits. It applies only to commercial transactions. It does not apply to wills and trusts; family law matters such as marriages, adoptions or divorces; court documents; or notices of termination of various sorts such as evictions, utility cutoffs, product recalls, and insurance cancellations. Although it applies to the *Uniform Commercial Code* provisions for contracts and sales, and for written waivers, it does not apply to commercial paper, bank deposits and collections, letters of credit, warehouse receipts, investment securities, or transactions involving a security interest.

The law prohibits the states from imposing any particular standards of their own for electronic signatures. Congress wanted to allow the private sector to come up with workable standards that could evolve over time.

E-SIGN makes it much easier to conduct business and enter into agreements online. Nonetheless, these days, when you're on the phone or online, you need to pay special attention to what buttons you push.

–by Robert L. Ellis, Columbus attorney and former chair of the OSBA Digital Technology Law Committee; rellis@petersonellis.com.

The Federal CAN-SPAM Act:
Rules for Marketing by E-Mail

If you or your business market by e-mail, make sure that your e-mail marketing complies with the new federal “CAN-SPAM Act” or you could face potential stiff penalties. The CAN-SPAM Act, which is the short title for the “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,” took effect on January 1, 2004, in an effort by Congress to curb the growing problem with “spam” e-mails. The act gives Internet users the right to demand that a party stop sending them commercial e-mails. The act empowers federal agencies (primarily the Federal Trade Commission or “FTC”), state agencies, and Internet service providers to enforce its provisions. Such enforcement includes the right to seek money damages (for example, the FTC can seek fines of up to $16,000 per violation) or criminal prosecution against those who falsify headers, those who falsely create e-mail accounts or Internet addresses in order to send spam, and against those who retransmit commercial e-mails to conceal the origins of spam e-mails.

CAN-SPAM applies to commercial e-mail
The Act applies to all “commercial e-mail,” that is, e-mails that have the primary purpose of advertising or promoting products or services. The act applies against anyone who sends commercial e-mail, initiates or procures the sending of the e-mail, or who retransmits such e-mail. It means that you are, or your business is, responsible for the commercial e-mails sent on your behalf by a third party you had employed to assist you with e-mail marketing.

The restrictions in the CAN-SPAM Act do not apply to *transactional* or *relational messages*, which are e-mails sent to facilitate, complete, or confirm a transaction, or provide warranty or safety information for a product or service used or purchased by the recipient.

General rules on how to comply with the CAN-SPAM Act:

- Commercial e-mails must clearly identify that the message is an advertisement if you do not have prior *affirmative consent* from an Internet user to send such e-mails. Affirmative consent means that the e-mail recipient expressly agreed to receive a message either in response to a clear and conspicuous request for such consent or at the recipient’s own initiative.
- The commercial e-mail must allow the recipient to send a reply message or other “Internet-based communication” to opt out of future e-mails from the sender. The “opt-out” information must include the sender’s valid, physical postal address.
- The e-mail sender can offer a list or menu that allows the recipient to choose which types of commercial e-mails would not be welcome, *provided* that this menu also includes a general opt-out of all commercial e-mails.
- The opt-out request must be honored with 10 days.
- The e-mail message must have correct header information.
- The message must have an accurate subject line. Avoid using clever turns of phrases in the subject line if such wording might confuse or mislead recipients regarding the content of the message.

Practical tips
The CAN-SPAM Act supersedes all existing state spam laws, except for state laws that prohibit falsity or deception in any portion of a commercial e-mail. For example, Ohio has enacted a statute that imposes criminal penalties against spammers who use fraud and deceit to send bulk

commercial e-mail in Ohio (ORC §2913.412). Therefore, a violation of the CAN-SPAM Act may violate Ohio law as well.

Your business should develop a reliable database system to collect, maintain and store customer information so that "unsubscribe" requests can be processed quickly, including all opt-out requests communicated directly to your business and to any third party engaged to assist with an e-mail campaign. It also means that your business must ensure that all opt-out requests provided to any third party are transmitted promptly to your business and to any other party managing your advertising e-mail database. Finally, this is not a comprehensive article on the CAN-SPAM Act; you should seek advice of your counsel on how you or your business should manage an e-mail marketing program.

–by A. Brian Dengler, a technology and intellectual property attorney with the Columbus office of Vorys, Sater, Seymour & Pease LLP. Updated by attorney Nancy L. Reeves of the Medina firm, Walker & Jocke.