LEGAL AND ETHICAL ISSUES
IN THE OPERATION OF A BUSINESS WEBSITE

SUSAN HIGGINS DEFAGO, John Carroll University
WILLIAM N. BOCKANIC, John Carroll University

The increasing importance of the Internet and the surging use of digital technologies are changing the business landscape in dramatic ways. This paper examines critical issues regarding how companies communicate with customers and many of the legal liabilities associated with these issues. The information provided targets primarily marketing managers of small to medium enterprises.

INTRODUCTION

In today’s business environment, the use of the Internet and World Wide Web is ubiquitous. Amazingly, the use of the Internet for commercial purposes (sales, advertising, etc.) only started in 1994. Originally funded by the National Science Foundation, the Internet operated for two decades restricted to relatively obscure government and university research network applications.

The speed with which this technology has been developed, adapted and accepted as a major component of business marketing strategy is astonishing. As a result, we have many great success stories in e-commerce, and probably an equal number of debacles. In the “early days” of commercial use of the Web, the popular press created a strong sense of urgency for marketing managers to get on-line or lose. “A media campaign without the Internet is suicide” (Himmelstein et al. 1997); “Internet Commerce is coming with hurricane force. As masses of companies turn towards it as a normal way of doing business, if you’re not there you’re going to be gone.” (Bylinsky 1992) Similarly, more recent predictions include meteoric increases in sales and advertising revenues from Web based enterprises (Jarvis 2002); and that the Internet will take over as the dominant medium for conducting market research (Jamieson 2002; Arnold 2004). It is estimated that business to consumer e-commerce sales will grow from $16 billion in 1999 to $5.7 trillion in 2004; business to business e-commerce is expected to reach $7.4 trillion in sales. (Kracher and Corritore 2004)

But as marketers move through the first decade of the 21st century, the dot.com bubble has burst and the U.S. economy is struggling to rebound from recession. New laws and regulations are tempering the ways technology can be used by marketers. The misuse of e-mail by spammers and privacy issues relating to identity theft leave consumers and businesses alike understandably cautious about the future in cyberspace.

Additionally, a growing number of articles related to serious legal and ethical issues must cause marketing managers to hesitate. Is Web marketing really something a business wants or needs? Also, just what are the rules in cyberspace? This paper will synthesize the consumer issues and attendant liabilities associated with marketing on the Internet, and offer a blueprint for rational decision making by marketing managers.

ISSUE: PRIVACY AND SECURITY

“Identity theft is the fastest growing crime in America today, impoverishing a third of a million households.” (Safire 2002) This stark statistic from the New York Times captures the essence of consumers’ fear of doing business on line. The basic problem is that consumers
feel they have no control over what happens to their personal information - where it is going, and how it will be used. One aspect of Web technology that is particularly troublesome to consumers is the use of cookies.

Cookies are “... tiny files that some Web sites place on your computer that serve as a tracking beacon. This site can then track your movements around the Web.” (Weber 1997) From a marketing manager’s perspective writing cookies is one way to gain a profile of its web site users in order to target advertising. “If you are an advertiser trying to analyze which Internet sites would reach your target audience, a simple list of Internet addresses is not useful. Cookies can be used by an Internet site to keep track of return visits, to build limited profiles of users and their activities on the host system (i.e. users who read the sports news are more likely to also visit the automobile classifieds).” (Coyle 2001)

The conventional argument in favor of the use of cookies is that cookies are actually a boon to consumers. They provide a personal touch to a Website: recognizing your browser each time you visit, providing services such as a shopping cart, assuring that you don’t see the same banner ads over and over again, and tailoring the ads you do see to your personal preferences. The information collected can actually guide the evolution of a Web site to become more customer oriented, perhaps offering customized products to individual shoppers. This argument seems to rely on the utilitarian principle of the greatest good for the greatest number. That is, the storing and selling of information actually benefits far more consumers (and businesses) than it harms. But from a consumer’s perspective, the fear is that their credit card number and other sensitive personal information is stored somewhere in cyberspace, and they have lost control of how, when, where and by whom it can be used. The problem is exacerbated by the ease with which information can be collected and cross processed with other information, potentially creating mega databases of very personal data. And while the government is prohibited from combining personal data across agencies by the Privacy Act of 1974, businesses are not.

While this may seem to be merely a nuisance, there are darker implications. “Few of us would feel free visiting alternative health treatment sites if we thought our medical insurers could obtain our Web surfing records, and job hunters would not want their current employer to be monitoring their visits to other companies’ sites.” (Coyle 2001) And new fuel for the privacy debate seems to turn up on an ongoing basis (Kanaley 2001):

So-called Web “bugs” and “e-mail wiretaps”- methods of placing hidden computer code in online images or certain types of e-mail to collect personal information.
The theft, allegedly by hackers, of private details on thousands of world leaders attending the World Economic Forum in Davos, Switzerland. The sale of data on schoolchildren’s Web-surfing habits by N2H2 Inc., a company that furnishes Web-filtering software to schools.

It is this central threat of fear, of not being told exactly what happens to the information provided, that has consumers distrustful of Web site transactions.

A lawsuit in Texas extends the accusation of cookies as a form of unwanted surveillance. This is a class action suit against Yahoo, filed under the Texas stalking laws, claiming that the use of cookies is a “surveillance-like scheme that monitors and stalks users without their full knowledge or consent.” (Kaplan 2000, p.2)

Currently, there are two factions wrestling with the privacy issue: those who favor strict federal regulation policing the use of personal information on the Web, and those urging effective industry self-regulation. In 1998, the Federal Trade Commission examined the use of privacy policies on the Web. In March of that year, the FTC conducted an audit of more than 1,400 commercial websites looking for evidence of
clearly stated and displayed privacy policies. Their findings revealed that 85 percent of the sites did collect personal information from consumers, but only 14 percent posted any privacy related notices, and only 2 percent posted a comprehensive privacy policy. (Cranor 1998, p.1)

What mechanisms exist for marketing managers contemplating a transactional Web site to assure customers that their privacy is protected?

**Hypothetical 1: Privacy Protection**

Ken Slick is the Marketing Manager of Sue-Us Sales, a medium sized distributor of electronic entertainment equipment. He has decided to include a Web site for the company to enhance its traditional marketing strategy. When John Naïve and Jane Leery enter the site they can click on any of the company’s product lines (stereos, big screen TVs, VCRs, etc.), read the description of features, what the price is and “experience” any of the items on-line. To make a purchase, simply supply name, address, phone and credit card number. To receive the one year unlimited warranty for free, simply click through the customer information warranty card on the screen.

John Naïve is hooked and orders a system with the free warranty. Three months later, however, he is disgusted with the deluge of offers (by mail, phone, and computer) to extend his warranty and buy more electronic equipment. He is considering filing a class action lawsuit against Sue-Us Sales for invasion of privacy.

Jane Leery does not feel comfortable putting her Visa number on the computer, nor does she see why the warranty card should include information about her activities, interests or opinions. She leaves the site with a very bad feeling about Sue-Us Sales.

How can marketing managers optimize use of the Web and effectively allay consumers’ fear of misuse of information?

**Recommendation 1: Be upfront and ask for permission.**

When designing a Web site, clearly state your company’s privacy policy before any information is collected. Then, simply ask your visitor’s permission as to how any information collected will be used. Many consumers enjoy getting additional information about a particular product class, and will not object to getting hooked up with other suppliers.

**Issue: Opt-in or Opt-out?**

Most businesses do now provide access to their privacy policies on line. Concerned customers can click on the privacy link and learn what the company does with any personal information collected. However, there are two approaches that may be employed to “get permission” from the consumer to use the information in the ways explained within the policy.

**Hypothetical 2: Informed Consent**

Ken Slick knows that he needs to put a privacy policy on the Sue-Us Sales site. He constructs the policy so that the first several hundred sentences are reassuring the visitor how much the visitor means to the company and how much it values the customer’s trust. The sections at the end of the policy tell the visitor that Sue-Us Sales “shares” your information with “our corporate family” and with non-affiliated parties for marketing purposes. After many pages of reading, the policy tells you that if you wish to “limit” this sharing of information, all you need to do is write to Sue-Us Sales giving your name, address phone number and account number. Finally, the policy warns that if you prefer to limit the use of your information by Sue-Us Sales, you will not receive offers for products and services provided by other companies that could help you lower costs, improve your finances and enhance your life.

Across town at Careful Sales, marketing manager John Forthright constructs his company’s privacy policy. It is written very concisely, in easy to understand language. The policy de-
Legal and Ethical Issues . . . .

Describes how Careful Sales uses cookies, and even offers instructions on how to turn them off, if that is the visitor’s preference. The policy clearly identifies other companies that Careful shares information with. The policy ends with a request to retain your information and requires the visitor to check a box if the visitor agrees.

Recommendation 2: Use an opt-in strategy for your privacy policy. In the long-run your respect for the individual customer will build trust and repeat business.

European companies tend to support the opt-in strategy. In fact it is the law in Austria, Germany, Denmark, Finland and Italy. To date, U.S. companies have preferred the opt-out approach. This is supported by the Direct Marketing Association in their Guidelines for Ethical Business Practices. (Kracher and Corritore 2004) However, this appears to be changing as Vermont now requires financial institutions to use opt-in, and 14 other states have opt-in privacy bills pending. California has passed a law requiring companies doing business with California residents to disclose what affiliated businesses they share information with. If they fail to disclose, the individual can sue for civil penalties up to $3,000 and attorney’s fees.

Several watch dog groups exist to help companies implement and maintain responsible online information gathering. Online Privacy Alliance is a group of more than 50 corporations and associations, including the American Advertising Federation, dedicated to protecting consumers’ privacy on-line. In order to be a member, companies must adhere to a set of guidelines designed to enhance privacy policies and safeguard the privacy of children. Additionally, third party organizations like the Better Business Bureau Online and TRUSTe are developing “seal” systems. Only those sites that commit to very stringent policies regarding the collection and use of private information are awarded the right to display the seal on their Web sites. According to a press release by BBBOnline, “... the purpose of the seal program is to serve as an available accountability mechanism that will demonstrate that your business stands behind its privacy policy. The BBB and other third-party organizations offer seal programs to indicate that a Web site is in compliance with recommended guidelines and practices, and to provide opportunities for dispute resolution.” (BBBOnline 2003) A seal program, monitoring the enforcement of privacy policies and having the authority to grant or revoke a seal, should let consumers know that a company’s privacy policy is enforced.

Marketing managers, in overseeing their company’s website as part of an overall integrated marketing communications plan, may be wise to consider the ethics involved in the collection and use of customer data. “Any form of deception or withholding of information is incompatible with maintaining the requisite context for legitimate communication.” (Drake et al. 2000). At the core of the marketing concept is the importance of building trust between provider and customer, with a focus on long term loyalty rather than short term sales. Any abuse of information technology can have a devastating impact on the company’s reputation, and limits the amount of trust it can foster, not only with customers, but with employees, stockholders and channel members.

LEGAL LIABILITY ISSUES

From a historical perspective, businesses have been involved in commonly accepted methods of marketing products and services, and, as a result, are both cognizant and comfortable with general marketing principles. The advent of high-tech methods of marketing goods and services, particularly the utilization of the World Wide Web as a marketing device, has propelled many businesses into substantially unexplored frontiers. By merely operating a Website, business organizations have been subjected to unfamiliar rules governing publishers, and the concomitant somewhat uncertain and potentially dangerous legal risk. Further exacerbating the danger is the fact that the laws of cyberspace, including both civil and criminal dimensions, are in a state of relative legal infancy and cur-
Legal and Ethical Issues . . . .

tently just beginning to be addressed by federal and state legislatures, as well as by the courts.

This section addresses several issues that make up this increased risk including copyright and their infringement, defamation, appropriation of a name or likeness, and Web site development contracts.

Copyrights -- General Background

The drafters of the United States Constitution specifically accorded constitutional protection for authors and inventors to create works and inventions that would be beneficial to society, thus providing for copyright and patent protection as follows:

The Congress shall have power . . . To promote the Progress of Science and useful Arts by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries. (United States Constitution)

Although an author may have received copyright protection, the protection is not perpetual. The rules here are somewhat complex but are briefly summarized in Appendix 1. To provide complete protection, works published before March 1, 1989 must bear certain notice or risk loss of copyright protection. The notice requirements are summarized in Appendix 2.

Copyright Infringement

Legal liability for copyright infringement may generally be divided into three major categories; namely, active or direct infringement, vicarious infringement, and contributory infringement.

Hypothetical 3: Direct Infringement

Sue-Us Sales locates a Web site created by Careful Sales. The Web site has creative graphics and outstanding text. Sue-Us Sales downloads the entire home page of Careful Sales and appropriates the Web site in its entirety. After a few appropriate changes of names addressees and other data, Sue-Us Sales registers its domain name and begins Internet sales.

The activity described here would be an example of direct or active infringement. Direct infringement involves the appropriation of the original creative work of another without permission. A business entity that incorporates materials such as text, pictures, graphics, software, or even sound into a Web site without permission of the owner of the work may very well incur liability for copyright infringement. The appropriation of digitized text such as would be viewed on a computer screen, digitized images (pictures), or digitized sound, rather than hard copy text from a book or magazine, a photograph from a photographer’s collection or a recording from a cassette tape, video tape or record would create no real distinction in terms of legal liability. If the business wishes to incorporate pictures, text, sound bytes or video clips into their Web site it is imperative that the business obtain in advance the express written permission of the copyright holder. While the copyright holder may have granted permission for use of the copyrighted material in one medium of expression such as print, further permission may not have been granted to use those materials in another medium of expression, such as digitized text, graphics, video or sound bytes on a Web site. Violation of copyright law could subject the violator to severe criminal penalties, as well as civil suit.

Recommendation 3. Be certain to obtain a comprehensive written grant of permission from the holder of any copyrighted work.

The permission should include all forms in which the copyrighted work is to be used, including digitized text, video and sound bytes, as well as multimedia compositions. Also, display digitized and written attribution to the creator of text, photos, graphics, or multimedia pieces when publishing these pieces on the business’s Web site.
Legal and Ethical Issues . . . .

Hypothetical 4: Vicarious Infringement

Arnold Appropriator, a marketing manager at Sue-Us Sales, locates an excellent sales training tutorial on the Internet. He downloads a segment of the article from the author’s Web site and then with the help of the Sue-Us Sales Webmaster, uploads it onto his home page on the business’s Web site. The management at Sue-Us Sales is unaware of Arnold’s actions, and his failure to obtain permission for use from the holder of the copyright.

This action may meet the requirements of vicarious (indirect) infringement, which may occur when a business establishes a Web site and exercises control over its content. By the appointment of a Webmaster (who is charged with the duty of approving all material that is to be uploaded onto the Web site) the business may incur liability for copyright infringement based on the theory that by controlling the content of the Web site, the business is thus acting as a publisher, such as of a newspaper or magazine, rather than a mere distributor of material such as a newsstand or public or private library.

In this fourth hypothetical, Sue-Us Sales, by assuming control of content, could incur legal exposure resulting from copyright infringement for material uploaded by employees or even visitors to the Web site. Businesses as “publishers” may be liable whether the copyright infringement was a result of the intent or mere negligence, on the part of the contributor of the material. Damage awards in such cases could be substantial. Of course, one could argue that the business could sue the visiting contributors for indemnification and, legally that may be so, provided the business can find them. Furthermore, if the contributor is an employee the employee’s assets ordinarily will be insufficient to make pursuing a lawsuit worthwhile. Thus, the likelihood that the business will seek indemnification from an infringing employee is relatively low. The usual course of action here would be termination of the employee, which will do nothing to help the business recoup a significant adverse damage award.

Recommendation 4. Make certain that the Webmaster regularly views and maintains control of the Web site.

This can prevent the unauthorized uploading of material that may infringe on the copyrights of others. Do not allow links to appear on the business Web site unless the linked site has given written permission to do so, and unless the business is certain that the linked sites do not themselves infringe on copyrighted material of others.

Hypothetical 5: Contributory Infringement

Sue-Us Sales maintains a business Web site, but does not employ a Webmaster or employ any security measures to prevent others from gaining access to its Web site. Furthermore, Sue-Us Sales takes no measures to control the Web site’s content. In an effort to provide high-tech service to its employees, Sue-Us Sales allows employees to create personal home pages and post them on the business’s Web site. One such employee’s creative home page provides a link to an off-business site that contains numerous marketing seminar materials that have been placed on that site in violation of the publishers’ copyrights.

Contributory infringement may thus occur where the business fails to exercise sufficient control over the contributions by others to its Web site. Therefore, in the above example, if the business allows others to freely upload material that infringes on copyrights or even links to other sites which themselves might be infringing on the copyrights held by others (or copyrights held by the linked site itself), the business might be held liable for contributory infringement due to its own negligence (i.e. lack of appropriate supervision or care). As one can see control over the content of a Web site is a two-edged sword-- the exercise of too much control may cause the business to be held liable as a publisher, and the exercise of too little control may result in the business being held liable for contributory infringement.
Legal and Ethical Issues . . . .

Recommendation 5. Do not allow employees to upload material to the business Web site.

Any material placed on the site should be done under the strict control and approval of the Webmaster. Do not permit employees on their personal Web pages to provide links to other Web sites.

Defamation

Defamation consists of publishing untrue, unprivileged material that injures the reputation of another. Defamatory material may be classified as slander where the defamation is oral, and libel where the defamation is written. Defamatory material published on a Web site would best be classified as written and, therefore, libelous even though such material is in digitized form.

Hypothetical 6: Libel

Sales rep Lucy Libel places a picture of Sales Manager Edwin Elderly on her personal employee Web Page of Sue-US Sales. Materials next to the picture state that employees should transfer to Mr. Elderly’s department if they don’t care if their boss is suffering from dementia, habitually late to work, managerially incompetent, and has given no bonuses for the past forty years. Additionally, copies of Mr. Elderly’s personnel records are available on the Web site by clicking on the appropriate hypertext link.

In our sixth hypothetical, Mr. Elderly is not, in fact, suffering from dementia. He has been late to work only once in the past twenty years, and that was because he was trying to help an employee who whose automobile was stuck in snow in the company parking lot. Additionally, Mr. Elderly recently won the “Outstanding Training Award” for excellence in sales training and management and has been relatively generous in awarding bonuses based on performance. Actually, Lucy Libel was dismissed from Mr. Elderly’s sales team because of excessive absences and consistently poor performance. Lucy Libel would certainly be liable to Mr. Elderly for the tort of defamation—specifically libel. Furthermore, because the business established a Web site with an employee Web page, gave employees authority to place material on that page, and also created a position of “Webmaster,” Sue-US Sales could possibly be vicariously liable to Mr. Elderly for defamation as detailed above.

Recommendation 6. Do not give employees uncontrolled access to personal Web pages.

No material should be placed on the Web pages without the advance approval of the Webmaster. Preferably, the Webmaster should be the only administrative individual given access to the Web site, including any personal home pages of employees.

Appropriation of Name or Likeness

In addition to the unauthorized use of a copyrighted picture, using a person’s name or likeness (picture or caricature) without permission may also be actionable as a tort and subject the appropriator to liability for civil damages (Restatement Second of Torts §652C).

Hypothetical 7: Appropriation of Employee Images

This hypothetical features Billy, the head of maintenance, and Mona, an intern at Sue-US Sales. While they were at the company picnic, they were photographed together in an amorous embrace. The company photographer took their picture without their knowledge or consent and uploaded it onto the “Employment Opportunities” section of the Sue-US Sales Web site under the caption “Make Life a Joyful Experience By Working for Sue-US Sales.”

Here, Billy and Mona may have a cause of action against both the photographer and Sue-US Sales for the nonconsensual “appropriation of their likeness and names.” The business, by failing to obtain a written photo release from the employees and placing their images on the World Wide Web, may be subjected to a possible cause of action for “appropriation of im-
age.” This action on the part of the business would constitute a form of invasion of privacy. Additionally, without first having obtained permission to do so, the inclusion in the Web site of names and/or pictures of individuals giving solicited or unsolicited testimonials about the organization’s products or services may also subject the business to liability for this tort.

Recommendation 7. Be certain to secure written permission from a photographer who holds a copyright on any images placed on the business Web site.

If the images captured are those of employees of the business, also secure written permission to use the images and/or names of the subjects from both the photographer and the subjects of the image.

Web Site Development Contracts

Business organizations often procure an outside consultant to perform the actual development of the Web site. Under U.S. Copyright law, absent an agreement to the contrary, if the designer of a Web site is a non-employee, ownership rights to that expression vest automatically in the person(s) who created it. Therefore, it is critical that there be a written agreement between the business and the external developer which vests ownership of the Web site and its entire content in the business. The writing should provide that any and all intellectual property rights in the Web site are exclusively owned by the business.

Notwithstanding that the business may use an employee or employees to create the Web site, it is important to specify that the Web pages are “work made for hire” and that the physical pages as well as all intellectual property rights accrue to the business. Among other things, the agreement should specify that the Web site developer transfers any and all electronic or display rights relating to text, photographic and graphical depictions, video, and interactive or multimedia rights to the contracting business. The agreement should be carefully drafted and sufficiently comprehensive to include all forms in which the creative object appears including digitized as well as traditional “hard copy” (i.e., print) forms. The business should investigate and have documentation that the developer has obtained rights in writing from the creator of photos, graphics sound bytes video, and text. Multimedia rights, as well as written permission from any subjects who might be featured or included in the Web site should also be secured.

Recommendation 8. Secure, in writing, all rights to the content, as well as the ownership of the Web site itself from the creator of the site.

The ownership of those rights should be clearly stated in the contract between the business and the Web site developer. If the developer is an employee rather than an independent contractor, the agreement should specify that ownership of any inventions, copyrights, or Web sites during employment—cr utilizing information obtained from the business or resources of the business—are considered to be work for hire and solely owned by the business. At the very minimum, this Web site development contract should detail the scope of the services to be provided, the due dates, and the dollar amount of any fees to be paid, as well as their payment schedule. Additionally, this agreement should stipulate that any and all copyrights to the creative work, including print rights and electronic or display rights, should remain the property of the business. Finally, in some cases it may be appropriate to maintain confidentiality about the Web site’s content until public unveiling is made.

Intellectual Property Protection

Any intellectual property posted on the Web is subject to being easily copied in its digital entirety. There are several policies, which, if followed, will at least discourage simple infringement. Internet surfers should be informed of the business’s copyright claim by placing an appropriate copyright notice on the business’s Web site. This notice is no longer required by law to assert a subsequent copyright infringe-
Legal and Ethical Issues . . .

ment claim, but it puts all Web site visitors on notice that permission is required for further distribution.

This copyright notice should appear at least on the home page of the business’s Web site, and the better practice would be to include it on every page. Some contractual arrangements with content providers may require the business to display certain copyright notices in addition to the one discussed below. In order to be effective as an infringement deterrent, the notice should embody the following aspects (Gillen 1996):

1. The word copyright, an acceptable abbreviation, or the symbol â. However, since not all Web browsers accurately depict the symbol’s ASCII code, perhaps the safest course is to use both; and
2. The year of first publication; and
3. The name of the copyright claimant; and
4. The statement All rights reserved.


Security

Several important features of a successful Web site are that it be attractive and dynamic, serving as an invitation for visitors to return frequently. One mechanism for providing that dynamism is to maintain an open policy allowing members of the business community to add content continuously. However this flexibility with respect to Web site content may be troublesome if tight security is not maintained with respect to other business computer systems including administrative systems, employee records and research databases. The data in these business systems may be exceptionally sensitive and an elevated degree of security must be maintained to keep Web site visitors from gaining access to these systems. One approach is to completely segregate the external Internet systems from the internal Intranet systems. Another approach includes security provided through the combination of hardware components, software components and human inter-

vention. Whichever approach is chosen, the business should carefully monitor the system for potential exposure. To avoid liability issues regarding copyright infringement or defamation, the Webmaster must exercise strict control of any content that is allowed to be added by members of the business community.

Recommendation 10: Through the use of firewalls, anti-virus defenses, and other state of the art hardware and software protection, maintain the highest degree of security between the Web site and other sensitive internal computer systems of the business.

Maintain strict control of any content added to the Website by others.

CONCLUSION

Although many potential legal liability issues were discussed in this paper, Web sites that minimize, if not completely eradicate, those risks can be constructed. The Web site should be planned with serious attention to the consumer and legal issues that make up such risk. The authors have addressed many of these issues in a set of recommendations on consumer issues and managerial controls that have appeared throughout this article and should accompany the building of a business’s Web site. These recommendations are summarized below:

Recommendations

- **Recommendation 1:** Clearly state how information submitted to the business web site will be used. Have the consumer grant permission that he/she has read the policy and consents to the use of the information as specified.
- **Recommendation 2:** Use an opt-in strategy rather than an opt-out one with regard to the business’s privacy policy. The consumer will be more comfortable that they are given the opportunity to consent to the terms of the privacy policy and use of information rather than feeling pressured or tricked into having to opt-out.

Marketing Management Journal, Spring 2006
• **Recommendation 3:** Be certain to obtain a comprehensive written grant of permission from the holder of any copyrighted work. The permission should include all forms in which the copyrighted work is to be used. Also, display digitized and written attribution to the creator of text, photos, graphics, or multimedia pieces when publishing these pieces on the business’s Web site.

• **Recommendation 4:** Make certain that the Webmaster regularly reviews and maintains control of the Web site to prevent the unauthorized uploading of material that may infringe on the copyrights of others. Do not allow linking unless the linked site has given written permission to do so. Be sure that the linked sites do not themselves infringe on copyrighted material of others.

• **Recommendation 5:** Do not allow employees to upload material to the business Web site. Any material placed on the site should be done so under the control and approval of the Webmaster. Do not permit employees on their personal Web pages to provide links to other Web sites.

• **Recommendation 6:** Do not give employees uncontrolled access to personal Web pages. No material should be placed on the Web pages without the advance approval of the Webmaster. Preferably, the Webmaster should be the only administrator given access to the Web site including any personal home pages of employees.

• **Recommendation 7:** Be certain to secure written permission from a photographer who holds a copyright on any images placed on the business Web site. If the images are taken by those in the employ of the business, secure written permission to use the images and/or names of the subjects.

• **Recommendation 8:** Secure in writing all rights to the content as well as the ownership of the Web site itself from the creator of the site. The ownership of those rights should be clearly stated in the contract between the business and the Web site developer. If the developer is an employee rather than an independent contractor, ownership of any inventions, copyrights, or Web sites during employment or utilizing information obtained from the business or resources of the business are considered to be work for hire and solely owned by the business.

• **Recommendation 9:** Display an appropriate copyright notice on the business’s Web site.

• **Recommendation 10:** Use firewalls, anti-virus defenses, and other state of the art hardware and software protection to maintain the highest degree of security between the Web site and other sensitive internal computer systems of the business.

This article, however, is not intended to be, nor should it be taken as the offering of legal advice or legal opinion. A variety of federal and state legislation, city ordinances, administrative regulations, judicial opinions, foreign laws, and even treaties may impact upon the operation of a Web site by a business for marketing or other purposes. Therefore, the authors caution the reader to seek competent legal counsel to address any issues of law that may arise in the construction and operation of a Web site.

**REFERENCES**


Legal and Ethical Issues . . . .


Gillen, S., “The Internet and Intellectual Property Law,” Presentation to Ohio Foundation of Independent Colleges Conference at Ohio Dominican College, Columbus, Ohio, October 4, 1996.


Restatement 2nd of Torts §652C (1977).


United States Constitution Article I Section 8, Clause 8.


APPENDIX 1
Copyright Protection

Copyright protection extends to “original works of authorship in any tangible medium of expression, now known or later developed “ (Title 17 Section 102(a) U.S. Code). When a work is published, it may bear a notice of copyright to identify the year of publication and the name of the copyright owner and to inform the public that the work is protected by copyright. Works that were published before March 1, 1989, must bear the notice or risk loss of copyright protection. The form of notice for visually perceptible copies should contain all three of the following three elements:

1. The symbol © (the letter in a circle), or the word “Copyright,” or the abbreviation “Copr.”; and

2. The year of first publication of the work. The year date may be omitted where a pic-


3. The name of the owner of copyright in the work, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner. (Copyright Basics)

**APPENDIX 2**

**Terms of Copyright Protection**

<table>
<thead>
<tr>
<th>Works Created Before but Not Published or Registered by January 1, 1978</th>
<th>Works Created Before and Either Published or Registered by January 1, 1978</th>
<th>Works Created on or after January 1, 1978</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life of the author plus 50 years.</td>
<td>28 years plus a renewal term of 28 years (Total Protection 56 Years).</td>
<td>Life of the author plus 50 years</td>
</tr>
<tr>
<td>Joint Works -- 50 years after the death of the last surviving author.</td>
<td><strong>If Copyright was secured from January 1, 1964 through December 31, 1977, Term is 28 years plus a Renewal Term of 47 Years (Total protection 75 Years).</strong></td>
<td>Works for Hire and Anonymous or Pseudonymous Works (unless author’s identity is revealed in the Copyright Office Records) 75 years from publication or 100 years from creation, whichever is shorter.</td>
</tr>
<tr>
<td>Works for Hire and Anonymous or Pseudonymous Works (unless author’s identity is revealed in the Copyright Office Records) 75 years from publication or 100 years from creation, whichever is shorter.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
