HANDBOOK OF E-BUSINESS

Editor

Jessica Keyes

New Art Technologies

RIA/WG&L

Boston • New York

E1

Building a Legally Bulletproof Web Site

TAMARA PESTER
LHS Group

DAVID TESKE
Alston & Bird LLP

Contents

PART D
The Financials of e-Business

PART E
The Sociological Aspect of e-Business

PART F
The Technology Behind e-Business

E1.01 INTRODUCTION

e-Commerce is changing the nature of business and introduces a special set of legal considerations to business transactions. Traditional commerce occurs when a business sells a good or service to a customer. Commerce includes the exchange of information, the exchange of funds, and the flow of goods. When any one of these commerce functions happens electronically, a business engages in electronic commerce.

A business transforming itself from bricks and mortar to clicks and mortar with an Internet presence through an e-commerce-enabled Web site must take several issues into consideration before laying the foundation (or connecting the cables) of its on-line business. Obtaining a sound mechanism for creating and enforcing binding contracts in electronically enabled mediums of commerce and diligently examining the particular issues that may be associated with building its on-line marketplace for goods or services will act as the best armor against legal bullets that others may aim at the business in the future. The careful businessperson will ensure that visitors to his or her Web site are aware of the terms and conditions of use, carefully construct a privacy policy, and take steps to protect his or her business's intellectual property, respect the intellectual property rights of others, and maintain awareness of other emerging legal issues associated with e-commerce. A Web-site audit, conducted either internally or by outside legal counsel, should review these issues to seal all legal holes before a Web site is launched.

E1.02 REQUIREMENTS FOR CREATING ENFORCEABLE CONTRACTS IN ELECTRONIC COMMERCE

Parties involved in e-commerce communicate electronically and might not communicate in traditional ways such as face-to-face meetings or the exchange of physical contracts. An e-commerce transaction may just as easily occur between strangers in different hemispheres as next-door neighbors. Electronic-commerce transactions take place over open networks, such as the Internet, or closed systems, such as dedicated electronic data interchange (EDI). The security and privacy of these transactions rely on various technologies.

Four items must be present for an enforceable transaction to occur: authentication, document and message integrity, privacy/confidentiality, and nonrepudiation. Authentication involves knowing the parties to the transaction. Document and message integrity means certainty that the document agreed to or the message sent has not been altered or modified. Additionally, the privacy or confidentiality of the transaction and acceptance or nonrepudiation of the transaction must be certain. In other words, to have an enforceable contract, a business must present evidence that:

- The contract it seeks to enforce is the contract the customer entered into and
- The customer "signed" the contract and
- The customer intended to enter into the contract and be bound by its terms.

A signature, whether in pen and ink on a traditional contract or an electronic signature in electronic commerce, plays several key roles. It plays an evidentiary function by authenticating and attributing the signer to the signed document. It plays a ceremonial function by calling to the signer's attention the legal significance of his or her act. Finally, it shows approval by expressing the signer's intention to give the signer's act legal effect.

To play the same roles in electronic commerce, an electronic signature must meet several criteria. It must show signer authentication by being unique to the signer. As in the physical world, the relying party may need assurance such as a notary, identification, or signature guaranty. The electronic signature must show document authentication by identifying what is signed and showing the impracticability of falsifying or altering either the signed document or the signature. Privacy and confidentiality concerns will be met if the message is sent over the Internet in an encrypted digital envelope. Nonrepudiation will occur naturally if the parties follow the steps just detailed. The use of credit cards can satisfy these requirements many times, as may a PKI (public-key infrastructure), a system of public-key encryption using digital certificates from registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. PKI systems are currently evolving and there is no universally accepted PKI or even a single agreed-upon PKI. Many Web sites use "clickwrap" agreements, in which a person signifies acceptance to viewed terms and conditions by clicking an "I accept" button. Unfortunately, no clear legal precedent exists recognizing the validity of the requirement of a legally binding clickwrap. However, nearly everyone agrees that reliable PKI systems are necessary before electronic commerce can become widespread.

E1.03 WEB-SITE TERMS AND CONDITIONS

Once the business has chosen a mechanism to ensure that the contracts entered into via its Web site will be binding, the company should ensure that visitors to its Web site are aware of the terms and conditions of use governing a visitor's use of the site. The businessperson and his or her attorney should consider the nature of the goods or services offered on the site, and draft appropriate terms and conditions. For instance, if the Web site includes bulletin boards, chat rooms, or other interactive areas, the business should consider including a provision detailing who owns what rights in posted material, an indemnification of the business in case the posted material infringes a third party's rights, guidelines detailing under what circumstances users' posted material may be removed, and when the business may deny access to certain users. Other standard provisions in a Web site's terms and conditions of use may include a warranty disclaimer to alert users that the business does not make any express or implied warranties regarding the timeliness of content on the Web site or the operation or uptime of the site; a limitation of liability; a description of the business's proprietary rights in the Web site; a disclaimer of any third-party Web sites to which links are provided; and a statement of the applicable governing law, jurisdiction, and venue in case of disputes.

Although most attorneys will probably counsel a business to include a statement of jurisdiction on its Web-site terms and conditions, recent developments indicate that the business's choice of jurisdiction might not be enforceable. The question of jurisdiction asks where an action can be brought based on the activities of the Web site. While the business's choice of jurisdiction may be enforced if its Web site is merely "passive," it may not be if the Web site is considered "active" or that the business is "doing business" through the Web site in several jurisdictions. A truly "passive" Web site merely posts content with no interactivity. An "active" Web site invites interaction by the use of a 1-800 number, an e-mail link, or some other means. A business is considered to be "doing business" in or with another jurisdiction when its Web site is a channel for purposely sending goods into interstate commerce intending or knowing that such goods will reach the subject state. Where jurisdiction is appropriate because of the degree of activity the Web site conducts, promises to be a question courts will continue to address. The results may vary as individual courts interpret the laws governing jurisdiction. The traditional measure of jurisdiction will almost certainly remain, though: the more contacts a business has with a particular forum, the more likely it will be subject to jurisdiction in that forum.

E1.04 PRIVACY

Not only will specifying the terms and conditions of use of a Web site help act as a shield to protect the business from claims by users, but posting and following a privacy policy will also help insulate the business from liability. Concerns about the use of individually identifying information continuously rank at or near the top of consumer worries. Some individuals wish to guard their identities while participating in frank discussions of sensitive topics. Others simply do not want each of their movements from Web site to Web site tracked by an invisible prying eye. Compounding these concerns are companies who track and store detailed user data, then resell the data to others wishing to target users with certain demographics. In February 2000, the Federal Trade Commission and the New York Attorney General's office announced that they were separately undertaking investigations of DoubleClick, Inc.'s, collection and use of data. Shortly afterward, DoubleClick indicated that it would not tie users' on-line activities to their off-line personal data until government and industry reached definitive privacy standards.

Sentiments regarding the protection of personal information have reverberated around the world. The U.S. Congress picked up on the wave of public sentiment and introduced over 100 bills regarding consumer privacy in the 106th Congress. On February 3, 2000, the European Union Data Protection Working Party issued a recommendation endorsing the implementation of Directive 95/46 regarding the transmission and use of its citizens' personally identifiable information, which directly impacts U.S. companies' operations. Several member states, including Belgium, Denmark, Spain, Greece, Austria, Portugal, Sweden, and Finland have already adopted the directive in part or in whole.

A business considering privacy issues in connection with a Web site should be aware that state, national, and international laws might apply to or restrict the particular way the Web site chooses to use information. Consumers generally feel more comfortable navigating a Web site when that Web site includes a privacy policy detailing how the Web site collects, protects, and uses information it gathers, as well as any steps the user can take to prevent disclosure of individually identifying information. The prudent advisor will carefully draft a privacy policy, and then ensure that it is followed. Several organizations such as TRUSTe, the AICPA, and the Better Business Bureau (through BBB On-line) have developed third-party oversight seal programs to alleviates users' concerns about on-line privacy and certify that a specific site bearing its certification seal has policies in place that make it trustworthy and reliable with regard to consumer information.

As privacy concerns gain more media attention consumers and lawmakers alike will more closely scrutinize measures that on-line businesses take with respect to individually identifying information. One absolute to follow in this environment of increased scrutiny and skepticism about privacy is to follow a privacy policy once it has been drafted or risk consumer and potential legal backlash.

E1.05 INTELLECTUAL PROPERTY

Once the legal backbone of a Web site—contract mechanisms, privacy policy, and terms and conditions of use—has been put in place, the business new to e-commerce should make sure it obtains and protects its own intellectual property, and avoids the potential pitfalls associated with the on-line world. Unlike real estate (real property), intellectual property consists of the intangible items that add value to a business and includes domain names, trademarks, copyrights, and patents.

[1] Domain Names

A business should first identify an available domain name (e.g. goldfishfeed.com) and become the registrant of the domain, thus allowing the association of the business's Web site with the domain name. Thereafter, the business should consider the preemptive registration of additional domains that could be easily imitated. For instance, a business focusing on pet food supplies that has reserved goldfishfeed.com should also consider reserving the domain names goldfishfeeds.com, goldfishesfeed.com, goldfishfeed.net, and other URLs that a user might mistakenly enter when trying to reach the goldfishfeed.com destination. In addition, it should consider registering the domain names and variations for the products and services it sells. Although this involves an initial outlay of funds, it will prevent disputes with others claiming rights to those URLs, and thus save money down the line.

Until 1999, Network Solutions, Inc., of Herndon, Virginia, held a virtual monopoly on the issuance and maintenance of domain names in the .com, .net, and .org top-level domains. The Internet Corporation for Assigned Names and Numbers (ICANN) was then formed to assume responsibility for Internet protocol space allocation and domain-name-system management previously performed through third parties under contracts with the United States. ICANN has authorized additional registrars of domain names including AOL.com and register.com.

All authorized registrars must follow the Uniform Domain Name Dispute Resolution Policy (UDRP). The new policy changed the methods available for dealing administratively with domain-name disputes. The rules of procedure and practice under the new UDRP can be found at http://www.icann.org. The policy outlines a simple arbitration proceeding to which all domain-name registrants must submit upon challenges to one of their domain name registrations. A party may initiate a dispute proceeding if:

- The domain name at issue is identical or confusingly similar to a trademark or service mark in which the party has rights (this applies to federally registered marks and it appears to allow licensees to assert claims);
- The domain-name registrant has no rights or legitimate interests in the domain name; and
- The registrant registered the domain name in bad faith.

If either of the parties files an action with a court of competent jurisdiction during the pendency of a proceeding under the UDRP, the arbitration panel may suspend or terminate the administrative proceeding, or, in its discretion, proceed to a decision. No form of appeal exists under the UDRP. If the complainant wins, NSI will transfer the domain name to it. If it loses, its only recourse is to file suit. If the domain-name registrant loses, it too may file suit to prevent the panel from taking away its domain name.

Trademark owners who need immediate injunctive relief to address the actions of a domain-name registrant may still assert their claims in court. However, the UDRP offers a relatively quick, inexpensive method to obtain the transfer of a domain name in a clear case of cyberpiracy when trademark owners do not need immediate relief and the domain-name registrant has offered the relevant domain name for sale. ICANN's relatively easy and inexpensive proceedings may, in certain instances, weigh in favor of filing in federal court. Because of the greater burden and expense on the domain-name registrant of litigating in federal court, as well as the intimidation of being in front of a federal judge, the domain-name registrant may be less willing to fight federal court litigation than a UDRP dispute. Litigation in federal court will therefore continue to be a viable alternative in many cases, particularly if there is any concern at all about the strength of claims under the UDRP's requirements.

[2] Trademarks

Trademark rights should be considered before or during the initial selection of a domain name. Trademarks are identifying marks used in connection with goods; service marks are marks used in connection with the provision of services. Several steps should be taken with respect to these marks. The preliminary step involves clearance and investigation to ensure that the proposed mark is available for use and potentially available for registration with the U.S. Patent and Trademark Office (PTO). If so, the next step is to apply for federal registration, which will give others constructive notice of the business's ownership rights in the mark. Finally, trademark or service mark notices should be prominently displayed wherever the marks are used on the Web site. If a mark has achieved registration with the PTO, the symbol should be displayed; otherwise, the TM or SM symbols should be displayed in connection with trademarks or service marks, respectively.

Once a business has secured rights in the marks it has selected, it should be vigilant with respect to their use and possible infringement by others. Trademark infringement centers on the question of whether two marks are "likely to cause confusion" with each other. Marks are considered confusingly similar if the buying public would think that the products or services covered by the mark come from the same source or are affiliated with the goods or services covered by the previously used mark. The courts and the PTO have established factors to consider in determining whether a likelihood of confusion exists. Although the precise factors differ from jurisdiction to jurisdiction, they generally include:

- The relative strength of the plaintiff's mark;
- The similarity of the mark at issue;
- The similarity of the products or services covered by the mark;
- The types of purchasers or consumers;
- The advertising media use;
- The defendant's intent in adopting the mark; and
- Whether any actual confusion has resulted from the defendant's use of its mark.

The courts, the PTO, or juries weigh these factors to determine if a likelihood of confusion exists. If a business creates an alliance with another company or allows affiliated companies to display hyperlinks to its Web site consisting of its marks, it should be careful to supply them with trademark usage guidelines. Finally, a business should not only be vigilant with respect to its own trademarks, it should also include correct attribution of other's marks, if any, on its Web site.

[3] Copyrights

Copyright protects original works of authorship, including literary, dramatic, musical, and artistic works such as poetry, novels, movies, songs, computer software, and architecture. Copyright does not protect facts, ideas, systems, or methods of operation, although it may protect the way these things are expressed. Copyrights are self-executing; that is, a work receives copyright protection the moment it is created and fixed in a tangible form so that it is perceptible either directly or with the aid of a machine or device. Although no requirement exists to register works with the U.S. Copyright Office, the Copyright Act provides several inducements or advantages to encourage copyright owners to register their works. Registration may be made at any time within the life of the copyright, and offers advantages, including the following:

- Registration establishes a public record of the copyright claim.
- Before an infringement suit may be filed in court, registration is necessary for works of U.S. origin.
- If made before or within 5 years of publication, registration will establish prima facie evidence in court of the validity of the copyright and of the facts stated in the certificate.
- If registration is made within 3 months after publication of the work or prior to an infringement of the work, statutory damages and attorney's fees will be available to the copyright owner in court actions. Otherwise, only an award of actual damages and profits is available to the copyright owner.
- Registration allows the owner of the copyright to record the registration with the U.S. Customs Service for protection against the importation of infringing copies.

Because two clicks of a mouse can cut and paste just about anyone's copyrighted work that is displayed on the Internet, it has earned the unfortunate nickname of the "World's Largest Copying Machine." To avoid claims of copyright infringement, a business must have rights to use the content of its Web site. It will have rights if the content was created by an employee, unless a written agreement between the business and the employee specifically states otherwise. In contrast, if an independent contractor created content for the business, that individual will own the copyright unless an agreement specifically states otherwise.

[4] Patents

Patent rights have become increasingly important to Internet businesses. The triggering event was the *State Street Bank* decision, which validated patent protection for "business methods." A business-method patent provides an enforceable monopoly to operate a business in a particular manner. Usually this is described in a series of steps. Well-known examples of business-method patents in the Internet space are the Amazon.com 1-Click patent and the SBH "shopping cart" patent. Amazon.com acquired patent rights on its 1-Click checkout method in which a shopper's profile information including credit card and shipping address are stored by a business and then automatically retrieved and utilized when that user wishes to check out and purchase an item. Amazon.com has successfully used this patent in litigation to force its main competitor, barnesandnoble.com, to remove a similar feature from its site under a preliminary injunction just prior to the 1999 Christmas season. Accordingly, business-method patents, and other patents, can be used in an offensive manner. Patents can also be used defensively in the Internet space by validating a company's use of a particular method against another entity that might claim infringement. Finally, investors increasingly expect and require Internet businesses in which they infuse funds to have either patent applications or patents covering their core technology as a factor, potentially determinative, in funding the company.

E1.06 FTC ACT VIOLATIONS, FALSE ADVERTISING, AND UNFAIR COMPETITION

Many companies fail to realize that the statements they make on their Web site are subject to Federal Trade Commission (FTC) regulations and the common-law theories concerning false advertising and unfair competition. Any Web-site review should therefore consider the veracity of statements made on the site. The FTC has authority to investigate an Internet-based business and require that it provide the "reasonable basis" under which it makes advertising statements. For example, the FTC may find fault with a company for claiming that its services are the "fastest" or that transactions between a consumer and the company via the Internet are "absolutely secure." The FTC is actively performing such enforcement with respect to Internet companies. One particular example is its investigation into DoubleClick Inc.'s activities concerning the collection of consumer data.

Claims of false advertising or unfair competition can easily arise on the Internet. For example, a claim might arise out of the use of another company's logo. Many Web pages link to the Web pages of other companies. Depending on how the linking is done, the linked-to company could file an action arguing that the use by the linking company's Web site of its name or logo improperly implies a connection between the two companies, or an endorsement of the linking company by the linked-to company. Accordingly, Internet companies must make sure they have appropriate clearance to link to other companies' Web sites.

Finally, because the Internet is a worldwide communication method, a company may find itself defending an action brought under foreign laws or by foreign regulatory agencies. For example, advertising regulations in the United Kingdom prevent comparative advertising. However, comparative advertising is a standard practice among American companies.

E1.07 DEFAMATION

Thousands of people interact with each other through bulletin boards, chat rooms, usenet newsgroups, and elsewhere on the Internet. Like all places where people congregate and communicate, these on-line communities may serve as forums where people are the subject of others' cruel words. The targets of such abuse have recently tried to hold the hosts of the on-line communities liable for defamation occurring in or on the hosted areas. Recent case law and legislation have addressed the question of the extent to which the hosts may be liable for defamation, but have not provided consistent answers. Courts have considered several factors in struggling with this question. If an entity takes a more active role in monitoring or editing content posted on its hosted forum, a court is more likely to hold that entity liable. On the other hand, if an entity has no notice of the defamatory activity and merely acts like a traditional print publisher by disseminating information, it is less likely to be held responsible when information transmitted on or by means of its service is defamatory. Courts in the United States and abroad continue to wrestle with the question of when it becomes appropriate to hold such hosts responsible for the defamation. The best shield against a cry of liability for on-line defamation is a policy that is carefully crafted and consistently implemented to deal with any notification of defamatory activity occurring on a hosted area.

E1.08 CONCLUSION

Just as e-commerce opens up new avenues in which to do business and access to new markets, it also introduces new and emerging legal issues. A business entering into the world of e-commerce should conduct a thorough Web-site audit prior to allowing its first customer the opportunity to enter into its virtual marketplace. The audit should review the mechanism for creating enforceable contracts, Web-site terms and conditions, privacy, the spectrum of intellectual-property protection, compliance with FTC, False Advertising, and Unfair Competition standards, and on-line defamation. Once these issues have been fully vetted, the business can confidently engage in e-commerce.

E1.09 ABOUT THE AUTHORS

Tamara Pester and David Teske are attorneys focusing on intellectual property and technology law. Tamara (tpester@yahoo.com) is in-house counsel at LHS Group, a global telecommunications software company. She concentrates primarily on structuring and negotiating high-technology and Internet-related transactions. She received her J.D. in 1998 from the University of Denver College of Law and her B.A. cum laude in History from Washington University in 1994.

David (dteske@alston.com) is a member of the Intellectual Property transactional practice team at Alston & Bird, LLP, where he represents high-technology companies and larger end users of technology in technology transactions. He also counsels clients in all aspects of patent practice. David attended the State University of New York at Buffalo, where he earned his J.D. in 1993.