

WORKING PAPER

No. 01-03G

April 2001

“Taming the Wild West- Legal Issues for Web Site Operators”

By

Charles R.B. Stowe MBA, JD, Ph.D., Professor
and
Keith Jenkins JD, Associate Professor

Sam Houston State University
College of Business Administration

Copyright by Authors 2001

The Working Papers series is published periodically by the Center for Business and Economic Development at Sam Houston State University, Huntsville, Texas. The series includes papers by members of the faculty of the College of Business Administration reporting on research progress. Copies are distributed to friends of the College of Business Administration. Additional copies may be obtained by contacting the Center for Business and Economic Development.

Taming the Wild West – Legal Issues for Web Site Operators

Charles R. B. Stowe*
Keith Jenkins*

The internet has been described as the wild west – an almost lawless area where electronic pioneers are pushing new boundaries with their innovations. However, during the past ten years, as the “wild west” has received more settlers, demands for law and order have changed the legal landscape. In today’s environment, the operation of a web site is no longer totally unregulated. It is no longer prudent to design a strategic plan for exploiting this medium without considering the legal issues. This paper provides an overview of the legal issues, regulations, and litigation that is beginning to refine or place boundaries on ‘internet-related’ activities. The strategic implications of changing landscape of jurisdictional issues, intellectual property protection, contracting, electronic banking/payment systems are among the topics that should be addressed by managers in their strategic plans.

This overview does not analyze each legal issue or survey the entire scope of legislation. It’s purpose is to alert management and web site employees including programmers and technical people to the need to have a better understanding of the emerging legal environment. There are many issues that have yet to be resolved with certainty and some of these areas are identified. This brief glimpse at the cyberlaw landscape should serve to warn those who operate a web site or e-commerce business of the potential liabilities. It is now foolish to plan e-commerce strategies with an appreciation of the new “sheriffs” on the plains of electronic highways. Law professors who teach in colleges of business will find this article helpful in addressing the development of a curriculum for teaching cyberlaw. This article makes the argument that there is simply too much material to incorporate this area into an existing course and that we should be advocating the creation of a cyberlaw course requirement for all management information systems and e-commerce majors whether undergraduate or graduate.

* Charles R. B. Stowe MBA, JD, Ph.D, Professor, and Keith Jenkins JD, Associate Professor, Sam Houston State University, College of Business Administration.

Sketching the Changing Legal Landscape

The problem with attempting to present cyberlaw is that it is simply not possible to present a photo of the current state of the law. Those who teach real estate law, probate law, or the Uniform Commercial Code would pretty much agree that there is (1) rules that clearly establish jurisdiction, (2) a clear sense as to the primary 'source' of law, (3) a strong record of common law that explains or interprets relevant statutes, and (4) a basis for comprehending the underlying transaction. However, cyberlaw is characterized by (1) no single 'source' of law, (2) unresolved issues of jurisdiction, (3) relatively short history of published opinions, and (4) simply understanding the underlying transaction requires some degree of technical sophistication. Add to this the fact that the underlying technology is changing far faster than the regulators and legislators, and you have a blurry image of a landscape. Cyberlaw is changing as fast as a fast-forwarded video and there are lots of unresolved issues.

In some ways teaching cyberlaw is analogous to teaching international law. Like international law, there is no 'one' or singular source of cyberlaw. Regional organizations like the European Union are developing their own set of regulations.¹ Within the United States, Congress at the federal level has enacted many laws that have serious implications for web users. These laws range from disclosure of the use of information collected through web sites to taxation² to the organization of the internet³ to the validity of digital signatures.⁴ Federal government agencies in their regulatory role have issued regulations on on-line banking, advertising practices, and consumer protection issues. National organizations have proposed different laws for state

¹ See Burgunder, Lee Legal Aspects of Managing Technology, West Legal Studies in Business – Thomson Learning, 2001. pp. 41, 49-52, 515-16, 617-620.

² Cowling, David "Taxation of Interstate Transactions, Internet Services and Electronic Commerce" paper presented at University of Texas School of Law 12th Annual Computer Law Conference, Austin, Texas, May 12, 1999.

³ For an interesting history of the development of the internet see Thornburg, Elizabeth G. "Going Private: Technology, Due Process, and Internet Dispute Resolution" 34 *U.C. Davis L.Rev.* 151, Fall 2000.

⁴ 106 P.L. 229; 114 Stat. 464; 2000 Enacted S. 761; 106 Enacted S. 761 "Electronics Signatures in Global and National Commerce Act."

ratification relating to the enforceability of contracts over the world wide web. And, individual states have enacted laws ranging from criminal statutes to taxation of phone use to fund computer technology for public schools and universities.

However, there is also a big difference between the cyber environment and international transactions. Whereas international transactions have always been defined by a high degree of government regulation and oversight, the history of the world wide web technology though funded by the US Government Department of Defense. The original concept was to develop a communication system that would be impervious to military attack (by being able to route to thousands of online servers at universities and defense installations, and as a means to increase the value of DOD national defense research expenditures by encouraging academicians to share data and research. While funded by the Department of Defense, the internet was created and maintained by non-government organizations whose underlying philosophy was quite libertarian.

There is the temptation to simply define cyberlaw as a subset of Intellectual Property Law thus confining issues to copyright, trademark and patent law. However, this leaves out extremely important issues surrounding web page design, domain names, marketing law, computer privacy issues and computer security issues. E-commerce which includes business to business transactions (B2B) as well as retail sales to consumers pulls in issues such as warranties, consumer protection laws, privacy issues and even web page design. A fairly recent addition is m-commerce for mobile-commerce: the use of handheld organizers that have wireless internet connection capabilities.

Introducing Legal Issues

One strategy to developing a broad understanding of cyberlaw is to start with the web page – something that small business owners and students can easily relate to. One of the major attributes of the html language is the ease with which one can copy materials from existing web pages to insert into one's own design. Copying photos, drawings, animations, etc may involve copyright infringement.

Some web sites use a protocol to restrict access. Examples include the *Wall Street Journal* which requires a subscriber name and password. On October 28, 1998, President Clinton signed the Digital millennium Copyright Act (DMCA) which made major changes to US Copyright laws to address the digital world. Part I of the Act amends U.S. copyright law to comply with the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty. The result was to provide legal remedies against circumventing technological protection measures and tampering with copyright management information. The Act prohibits manufacturing or making available technologies, products and services used to defeat technological measures controlling access while at the same time providing reasonable exceptions for online service providers, to permit temporary copies of programs during performance of computer maintenance, and to encourage continued research.⁵

Much attention has been focused on the Napster saga – a story which began in 1999 when the Napster web site offered free file-swapping software on the Internet. With the Napster software, individuals could look up a centralized list of songs posted by other enthusiasts and without paying any fees could download the songs to their computer where they could then burn their own CD. Since 1999 over 38 million people logged on to take advantage of the free service.⁶ The result, music publishers claimed, was a drop in single CD sales in the year 2000 and multiple lawsuits that were recently consolidated.⁷ Because the firm completely ran out of money, they formed a strategic alliance with Bertelsmann AG, one of the plaintiffs in which they will develop a secure, fee-based file-sharing service distributing Bertelsmann's music catalog. Napster will receive a \$50 million loan, convertible into stock for the music publisher. The company may charge a \$4.95 monthly fee for downloading Bertelsmann's music library.⁸

In the early days of the internet, cyber –entrepreneurs registered for all sorts of domain names hoping for quick returns from commercial organizations wanting attractive domain names. The result was that some individuals registered domain names that were

⁵ Morrison & Foerster LLP, MEMORANDUM to Clients and Friends, as published by 12th Annual Computer Law Conference, University of Texas School of Law, May 20-21, 1999

⁶ Editorial "Sharing the Music" *New Jersey Law Journal*, January 15, 2001.

⁷ *In re: Napster, Inc. Copyright Litigation*, 2000 U.S. Dist. LEXIS 15493.

⁸ Godwin, Mike "Lawful Copies Bertelsmann Chose to Make Music Rather Than War with Napster" *The American Lawyer*, February 2001.

really trademarked names. In November 1999, Congress passed the Anticybersquatting Consumer Protection Act which created serious penalties for those deliberately registering domain names with a bad faith intent to profit by from legitimate trademarks.⁹

Another aspect of page design is whether the cite was created to attract children. If so, then the web designers need to be aware of the Children's Online Privacy Protection Act (COPPA). While the provisions concerning online pornography were successfully challenged,¹⁰ if the cite attempts to collect information from minors (defined as 13 years or less), parental disclosure and consent is required. The Children's Online Privacy Protection Act of 1998 (hereafter COPPA) carries both civil and criminal penalties of up to six months in jail and a fine up to \$50,000 per day when the violation is intentional. The Act provides for civil penalties of \$50,000 per violation and each day is considered a separate violation.¹¹

While anti-pornography statutes have been successfully challenged, government efforts to outlaw gambling on the internet have been upheld.¹²

Some web sites are no more than electronic billboards, passively disseminating information to those who click in. Others, however, are interactive and invite the potential customer to shop on-line. Such interactive sites raise other legal issues such as what constitutes a warranty, and whether the terms of the sale are consistent with deceptive trade laws both at the federal and at the state level. The issue of contracting over the internet is one of those issues that is unresolved. During the summer of 1999, the National Conference of Commissioners of Uniform State Laws adopted the Uniform Electronic Transactions Act as a national standard for electronic signature legislation.¹⁰ The proposed act applies to electronic records and electronic signatures relating to a

⁹ Burgunder, *op.cit.* p. 442. ft 72 "Congress passed the Intellectual Property and Communications Omnibus Reform Act of 1999 (S.1948), on November 19, 1999 as part of a consolidated appropriations packages, which was signed by the President on November 29, 1999 (Pub.L.No. 106-113). The relevant title within this act is called the Anticybersquatting Consumer Protection Act.

¹⁰ *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 1999 U.S.Dist. LEXIS 735; 27 Media L. Rep. 1449; 14 Comm. Reg (P&F) 1145

¹¹ 47 USCA Section 231 (a) (1-3)

¹² Keller, Bruce P. "The Games's the Same: Why Gambling in Cyberspace Violates Federal Law" published by 12th Annual Computer Law Conference, University of Texas School of Law, May 20-21, 1999.

transaction.¹³ The Act provides for quite a few exceptions including laws governing the creation and execution of wills, codicils, or testamentary trusts, major portions of the Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2 and Article 2A (meaning that rules relating to signatures for banking (Articles 3 and 4), secured transactions (Article 9), warehouse receipts, investment securities, etc are not covered. The act does not apply to other laws identified by the State (which may include specific consumer protection statutes, for example). Otherwise, the act broadly states that electronic signatures are valid and electronically generated contracts satisfy the Statute of Frauds. The electronic signature is defined as any Aelectronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.¹⁴ The significance of this provision is that the authors were trying to anticipate current and future technological developments for Avoice prints@ and other forms of signatures beyond that of an electronic version of a handwritten signature. The key element of whether an electronic signature is valid is whether the electronic record is capable of being retained by the recipient at the time of receipt. If the sender or its information processing system can inhibit the ability of the recipient to print or store the electronic record, then the transmission is not an electronic signature. The term Aelectronic signature@ includes facsimile, electronic mail, voice mail, audio, records, as well as internet transmissions both encrypted and nonencrypted. However, a critical element is that the party intended to make the signature. A mere click on AI agree@ will suffice to show intent. Even typing ones= name on an email message may act as a valid signature or applying a biometric or encryption technology to a message with the intention to sign is sufficient. The Act does not require a transmission to replicate a handwritten signature. While this may sound radical, recall that the UCC provides that a stamp or mark may serve as a signature.¹⁵ Courts have also concluded that names on

¹³ Uniform Electronic Transaction Act Section 3, Scope as posted at www.law.upenn.edu/bll/ulc/finact99/1990s/ueta.htm

¹⁴ Uniform Electronic Transaction Act Section 2, Definitions (8), as posted at www.law.upenn.edu/bll/ulc/finact99/1990s/ueta.htm

¹⁵ Uniform Commercial Code Section 1-201 (3) ASigned@ includes any symbol executed or adopted by a party with present intention to authenticate a writing.

telegrams, names on telexes, typewritten names, names on Western Union Mailgrams and even names on letterhead may serve as signatures.¹⁶ The Uniform Electronic Transactions Act takes a very liberal approach as to what is a signature that is consistent with the UCC and court cases.

The Act deals with the issue of what happens if there is a change or error in an electronic record during the course of a transmission. If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure but the other party hasn't, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may have the affect of the changed or erroneous electronic record. In the event that a third party Aelectronic agent@ is used, an individual may avoid the transaction if the electronic agent did not provide an opportunity for the prevention or correction of the error and if at the time that the individual learned of the error the individual promptly notified the other party that they did not intend to be bound by the electronic record, and they took reasonable steps to return or consideration received, and they have not already received any benefit or value from the consideration if any, received from the other person so long as they were created with intent.¹⁷

The federal government has recently stepped into the issue of electronic contracting. President Clinton signed Electronic Signatures in Global and National Commerce Act on June 30, 2000. The act eliminates legal barriers to using electronic technology to sign contracts, collect and store documents, and send and receive notices and disclosures. The Act requires that web page operators obtain consent from customers to doing business on-line and does not change any consumer protection laws. The Act also permits the electronic storage of documents that otherwise would have to be stored in warehouses.¹⁸ The effect of the law is to grant electronic signatures and documents equal legal standing with traditional handwritten signatures and written

¹⁶ Smedinghoff, Thomas J. & Bro, Ruth Hill AMoving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce@ 17 *J. Marshall J. Computer and Info. L.* 723.

¹⁷ Uniform Electronic Transaction Act, Section 10 Effect of Change or Error, as posted at www.law.upenn.edu/bll/ulc/finact99/1990s/ueta.htm

¹⁸ Office of the Press Secretary, The White House, June 30, 2000 on <http://clinton4.nara.gov/WH/New/html/20000630.html>

records, preempting state law to the contrary.¹⁹ Web designers must be aware of the disclosures and consent requirements in designing interactive web pages.

Once a transaction is entered, the next issue is how funds are collected. Web site operators have a variety of choices in terms of banks and third party collectors. The legal issues are significant as the issue of credit card companies and warranties can result in significant liability from 'charge – backs' from retail customers. The contracts between banks or electronic collection companies and vendors contain provisions that expose vendors to a certain degree of liability.²⁰

There are often a host of other contracts involved in developing a web site. These include contracts with Internet Service Providers (ISPs). There may be contracts with telecom companies providing internet connections (DSPs). Software to run the web page must be leased or licensed depending on whether the company is using its server equipment or using the services of a third party internet service provider. Warranties on downtime, capacity, service capabilities, etc. A corollary activity is maintaining an 800 number hotline. If tangible goods are provided, contracts may be signed to hire a fulfillment service.

Developing Issues

While the Congress passed the Internet Tax Freedom Act,²¹ this act has only deferred the issue of taxation of transactions over the internet for a three year moratorium. The Act bars state or local governments from taxing Internet access until October 21, 2001, bars state or local governments from imposing taxes that would subject buyers and seller of electronic commerce to taxation in multiple states, and establishes a temporary Advisory Commission of Electronic Commerce to study electronic commerce tax issues and report back to Congress after 18 months on whether electronic commerce should be taxed. However, any valid state or local taxes that existed prior to October 21,

¹⁹ Poggi, Christopher "Electronic Commerce Legislation – An Analysis of European and American Approaches to Contract Formation, 41 *Va.J,Int'L* 224, Fall 2000

²⁰ "The Legal Risks of Setting Up Shop in Cyberspace, 6 *Journal of Organizational Computing and Electronic Commerce* 51 (1996).

²¹ P.L. 105-277, included as Titles XI and XII of the Omnibus Appropriations Act of 1998; Approved as H.R. 4328 by Congress on October 20, 1998; Signed as Public Law on October 2, 1998.

1998 are grandfathered. This permitted Connecticut, Wisconsin, Iowa, North Carolina, South Dakota, North Dakota, New Mexico, Tennessee and Ohio to continue to collect taxes on internet access fees. Stick and brick retailers have tended to promote taxation of retail sales over the internet while purely internet or dot.com companies oppose any sales tax. As economic activity increases over the internet, state legislatures are going to find it an increasingly attractive target for taxation.

The issue of compliance with regional, national and local consumer protection laws is going to continue to evolve. There is a case involving a guarantee of customer satisfaction with return rights was found to violate German law which is designed to protect the “mom and pop” retailers from the larger retailers who are in a better economic position. LL Bean found out that when a German ordered some clothing from its web site, it fell under the jurisdiction of the German courts! Even in the United States, an entrepreneurial firm attempted to offer California wines through the internet only to find out that such “direct” sales violated a California law designed to protect liquor wholesalers. Early indication of jurisdictional issues suggest that world wide web may mean world wide liability for electronic vendors!!!²²

There are two important legislative initiatives before many state houses: the Uniform Electronic Transactions Act (UETA) and the Uniform Computer Information Transactions Act (UCITA). UETA has previously been discussed. UCITA is perhaps the more controversial proposal because it encompasses specific contractual rules relating to the behaviors of parties to a contract. The Uniform Computer Information Transactions Act only addresses those transactions involving the licensing of software, the use of internet-based data bases or distribution of information on the Internet.²³ The Act provides that parties may opt for having their contract treated under UCITA if they have had opportunity to indicate their consent after proper disclosure. Such consent may be included in software whereby an AI agree@ button is provided at the end of a licensing or contractual agreement. In the case of shrinkwrapped contracts, the provisions are a bit more controversial in that a customer may find that they have

²² Ferrera, Lichtenstein, Reder, August, Schiano *Cyberlaw Text and Cases*, West- Thomson Learning, 2001, pp. 22-24. Burgunder, Lee B. *Legal Aspects of Managing Technology*, West- Thomson Learning, 2001, pp 24-32.

²³ Shah, Patrik, “The Uniform Computer Information Transactions Act” 15 *Berkeley Tech. L.J.* 85 Annual Review of Law and Technology.

assented to the UCITA rules after they have purchased the software. UCITA provides a partial remedy in that the customer has the right to return the software or program for a full refund if they do not wish to be held under the UCITA rules.²⁴ Critics of UCITA note that the FTC's model for most state consumer disclosure laws requires that the merchandisers of shrink-wrapped software provide stronger disclosure when after-purchase contract terms are to be part of a contract than UCITA's rather liberal definition of the term conspicuous. UCITA describes conspicuous as a term so written, display or presented that a *reasonable person* (emphasis mine) against which it is to operate ought to have noticed it. The Act suggests that conspicuous terms include a heading in capitals in a size equal to or greater than or in contrasting type, font or color, to the surrounding text....²⁵

Critics also note that UCITA's language on warranties do not adequately protect consumers. Again, the issue focuses over UCITA's definition of conspicuous in that a party may disclaim implied warranties so long as such a disclaimer is conspicuous.²⁶ Another consumer protection problem is that UCITA's Implied Warranty of on accuracy of informational content does not cover published informal content.²⁷ There are really two aspects to computer based software, the engine and the content. For example, CD-ROM based encyclopedias contain programs to play content and the actual content itself. In one sense having this limitation on liability for content makes sense using an argument that has protected film processors from liability of loss. Recall that if a film processor loses one's film, they are limited to the cost of replacement of the film itself and not for consequential damages. The justification is that film processing would become prohibitively expensive if labs were liable for the cost of recapturing the images that were lost. If computer software providers were held liable for all potential damages arising from an error in content, the risk of liability might well discourage the use of electronic media for dissemination of information not to mention the First Amendment free speech arguments. On the other hand, where there is special reliance, publishers may

²⁴ UCITA 209 (b) and Comment notes.

²⁵ *Id.* 102 (14)

²⁶ *Id.* 406 (b)(1)(A)

²⁷ Shah, Patrik, *The Uniform Computer Information Transactions Act* 15 *Berkeley Tech. L.J.* 85, - Annual Review of Law and Technology.

be held liable for inaccuracies such as publishers of navigational charts.²⁸ And, issues over the potential liability arising from computer programs that may contain viruses are equally troubling to UCITA's critics.²⁹

UCITA also permits parties to treat Federal Copyright Laws as >default= regulations in that parties may contract to alter rights that are defined under federal statutory and common law. The justification is that digital programs have very different characteristics than traditional published materials. For example, the sale of a computer program for an individual's sole use is different than say authorizing them to use the program to perform services for others.³⁰ The legal debate over the issue of whether UCITA should permit parties to circumvent federal copyright provisions is based on a more basic dispute: to what extent should law promote the burgeoning information industry versus the issues of public domain as set by copyright law.³¹ Giving financial incentive to vendors who create both computer program >engines= and content may well spur e-commerce. On the other hand, why shouldn't the same rules for conducting business be the same whether they are transacted on and by paper or conducted electronically? These are the issues that will continue to haunt UCITA and slow its passage by the states.

There are other state laws that were not written for the purpose of restricting e-commerce, but have that effect. For example, many state franchise laws have the result of preventing automobile manufacturers from direct selling through the internet. While the major automobile manufacturers have extensive web pages, unlike the personal computer industry, customers cannot buy direct. Prior to engaging in setting up an e-retail operation, vendors should consider the implications of state and federal laws

²⁸ Ftn 78 and 79 in Shah, Patrik, *The Uniform Computer Information Transactions Act* 15 *Berkeley Tec. L.J.* 85, - Annual Review of Law and Technology.

²⁹ *Ibid.*

³⁰ Ftn 86 *See National Car Rental Syst., v. Computer Assoc. Int'l, Inc.* 991 F.2d 426, 432-33 (8th Cir. 1993) (holding that contractual restriction on processing of data for third parties constitutes an additional element distinguishing this cause of action from a copyright action)...@ in Shah, Patrik, *The Uniform Computer Information Transactions Act* 15 *Berkeley Tech. L.J.* 85, - Annual Review of Law and Technology.

³¹ Shah, Patrik, *The Uniform Computer Information Transactions Act* 15 *Berkeley Tech. L.J.* 85, - Annual Review of Law and Technology. AC. Which View is Right? Information Incentives vs. Public Domain Access@.

relating to their industry. Banking, insurance and other highly regulated activities are the obvious, but the earlier example of California's state law against selling directly from vineyards to electronic customers demonstrates how tricky this area can be.

The other area of law that is developing concerns spamming or the unsolicited selling of e-mail. Putting up a web page may be part of a firm's marketing program, but the world wide web is actually like an world wide electronic yellow pages where getting customers to visit the cite requires a lot of sales/marketing effort. Service providers such as America on Line have estimated that nearly one third of their e-mail traffic consists of spam or unsolicited e-mail. In cases where the solicitation offers an 'investment opportunity,' the issue of compliance with Federal Securities laws may be involved. In other cases involving legal services or medical advice, the issue may be one of defining what service is actually offered and whether the provider is properly licensed.

For service providers, the aggravation of spam is due more to drowning of their storage and mailing capacity than any inconvenience to their customers. Many states are confronting the issue of spam versus the issue of constitutionally protected commercial speech with various attacks on this practice. America On-Line has actually sued spammers on the basis of causing damage to their servers under the Computer Fraud and Abuse Act.³²

One of the great benefits of the computer is the ability to assemble huge databases as people 'visit' sites and often voluntarily provide information. Some web sites are designed as games or as lotteries whereby individuals wanting to play or a chance to win are asked to provide demographic information. Other sites collect information from customers who are 'registering' their product for service or warranty protection. The Collections of Information Antipiracy Act was introduced by the Clinton administration with the statement that "... information is the currency of our economic age. That puts a premium on designing a legal schema that creates sufficient incentives to maximize investment in data collection --- to expand the available university of information -- without putting in place unjustified obstacles to competition and innovation."³³ This

³² 18 U.S.C. 1030. See also Burgunder, *op.cit.*, pp. 537-538.

³³ Statement of Andrew J. Pincus, General Counsel, United States Department of Commerce before the Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, U.S. House of Representatives concerning HR. 354 "Collections of Information Antipiracy Act, 18 March 1999.

federal law provides parties who have created databases a private cause of action against those who misappropriate their database products. The U.S. is not alone in dealing with the issue of legal protection of databases as the European Union has also been drafting and issuing directives on the subject.³⁴

Peripheral Issues

Simply writing a web page is not equivalent to successfully building an e-commerce business. Office Max and Toys R 'Us provide two examples of brick and stick retailers who learned the hard way that the integration of different software systems with existing retail distribution and fulfillment centers is not as easy as it first appears. Both companies suffered substantial operating losses during their first year of operating their own web sites.³⁵ Arriving at a successful business model for e-commerce is going to require substantial investment in intellectual capital – employees which means that a peripheral issue for any organization is how to retain their investment in view of a fairly mobile labor pool. The issues of employment contracts and trade secrets therefore should become part of the legal strategy for companies engaging in e-commerce. There is considerable variation among states on covenants not to compete and the enforceability of employment contracts.³⁶

Another area related to the creation of “systems” or processes for managing e-commerce, m-commerce, B2B, etc is the issue of possible ‘business process patent protection.’ Priceline is not the only company to file hundreds of business process patents! Whether all these business process patents will be enforceable is uncertain, but aggressive filing is a strategy many firms have taken. The extent to which courts will recognize and enforce claims on these patents has yet to be resolved but early indications are that if and when certain business processes prove to be profitable, there will be lots of legal liability and litigation.

³⁴ Reichman, J.H. and Samuelson, Pamela “Intellectual Property Rights in Data?” 50 *Vanderbilt L.Rev.* 51 1997.

³⁵ See the Annual Report to Shareholders for the year 1999 and particularly the “Letter to Shareholders” of Office Max and Toys R 'Us for an interesting admission on the difficulties of selling via the world wide web.

³⁶ Claghorn, Holly “Employee Issues in the High Technology Sector ... Not to Compete and Other Delights” published by University of Texas School of Law for the 12th Annual Computer Law Conference, Austin, Texas, May 20-21, 1999.

Cyberlaw, Business Strategy, Education

The legal environment for those developing or operating in cyberspace is no longer the wild west where 'anything goes.' The sheer breadth of issues only briefly touched by this overview suggest that designing a business model or implementing a business strategy without considering the legal consequences can result in total business failure. Training future MIS or Computer Scientists on merely the technical capabilities of cyberspace without helping them develop some sensitivity to possible legal implications of their designs and strategies is irresponsible. Attempting to incorporate the wide variety of issues from contracts, to consumer protection laws, to taxation, privacy and jurisdictional issues into existing legal environment courses is not the solution either. The time has come when business schools should require a course in cyberlaw for all MIS, computer science and marketing majors both at the undergraduate and graduate level. While there are many areas of the law that are not resolved, presenting those issues to future e-commerce engineers and managers will at least sensitize them to seek preventive law advice thus perhaps saving their companies from expensive litigation.

